OPTIMIZE

MERCURY BUSINESS AVAILABILITY CENTER™

Configuring SiteScope Monitors

MERCURY™

BUSINESS TECHNOLOGY OPTIMIZATION

Mercury Business Availability Center

Configuring SiteScope Monitors

Version 6.1

Document Release Date: February 15, 2006

MERCURY™

Mercury Business Availability Center, Version 6.1
Configuring SiteScope Monitors

This manual, and the accompanying software and other documentation, is protected by U.S. and international copyright laws, and may be used only in accordance with the accompanying license agreement. Features of the software, and of other products and services of Mercury Interactive Corporation, may be covered by one or more of the following patents: United States: 5,511,185; 5,657,438; 5,701,139; 5,870,559; 5,958,008; 5,974,572; 6,137,782; 6,138,157; 6,144,962; 6,205,122; 6,237,006; 6,341,310; 6,360,332, 6,449,739; 6,470,383; 6,477,483; 6,549,944; 6,560,564; 6,564,342; 6,587,969; 6,631,408; 6,631,411; 6,633,912; 6,694,288; 6,738,813; 6,738,933; 6,754,701; 6,792,460 and 6,810,494. Australia: 763468 and 762554. Other patents pending. All rights reserved.

Mercury, Mercury Interactive, the Mercury logo, the Mercury Interactive logo, LoadRunner, WinRunner, SiteScope and TestDirector are trademarks of Mercury Interactive Corporation and may be registered in certain jurisdictions. The absence of a trademark from this list does not constitute a waiver of Mercury's intellectual property rights concerning that trademark.

All other company, brand and product names may be trademarks or registered trademarks of their respective holders. Mercury disclaims any responsibility for specifying which marks are owned by which companies or which organizations.

Mercury provides links to external third-party Web sites to help you find supplemental information. Site content and availability may change without notice. Mercury makes no representations or warranties whatsoever as to site content or availability.

Mercury Interactive Corporation
379 North Whisman Road
Mountain View, CA 94043
Tel: (650) 603-5200
Toll Free: (800) TEST-911
Customer Support: (877) TEST-HLP
Fax: (650) 603-5300

© 2006 Mercury Interactive Corporation, All rights reserved

If you have any comments or suggestions regarding this document, please send them by e-mail to documentation@mercury.com.

AMLIB_SISMONS6.1/01

Table of Contents

Welcome to Configuring SiteScope Monitors xvii
How This Guide is Organized xvii
Who Should Read This Guide xviii
Getting More Information xviii

PART I: WORKING WITH GROUPS, MONITORS, AND TEMPLATES

Chapter 1: Working with SiteScope Groups 3
About SiteScope Monitor Groups 3
Working with Monitor Groups 3
Configuring Group Settings 10

Chapter 2: Working with SiteScope Monitors 15
About SiteScope Monitors 15
SiteScope Monitor Types 16
Monitoring Remote Servers 19
Common Monitor Actions 25
Common Monitor Settings 31

Chapter 3: Using Templates to Deploy Monitors 43
About SiteScope Templates 44
Understanding Templates 45
Planning Templates 47
Creating Templates 48
Working with Template Variables 53
Counter Selection in Monitor Templates 60
Using Templates to Deploy SiteScope Monitoring 65
Exporting and Importing Templates 66

Chapter 4: Monitor Deployment Wizard....69
Monitoring Configuration Items with the Monitor Deployment Wizard....69
Using the Monitor Deployment Wizard....71
Configuring Settings for the Wizard....75
Template Reference and Monitor Tree Objects....75

PART II: SOLUTION TEMPLATES

Chapter 5: Introducing SiteScope Solution Templates....81
About Solution Templates....81
Working with Solution Templates....82

Chapter 6: Active Directory Solution Template....85
Understanding the Active Directory Solution....85
Deploying the Active Directory Solution Template....87

Chapter 7: Exchange Solution Templates....91
Understanding the SiteScope Exchange Solution....91
Deploying Exchange Solution Templates....94

Chapter 8: Oracle Solution Template....97
About the Oracle Database Solution....97
Deploying Oracle Database Solution Templates....99
Oracle Database Solution Tools....103
Understanding Oracle Database Solution Tools....103

Chapter 9: SAP Solution Templates....107
About the SAP Solution....107
Using the SAP R/3 Solution Template....108
Using the SAP J2EE Solution Template....111

Chapter 10: Siebel Solution Templates....115
About the Siebel Solution....115
Using the Siebel Application Server Solution Template....116
Using the Siebel Gateway Server Solution Template....122
Using the Siebel Web Server Solution Template....124

Chapter 11: WebLogic Solution Template....127
Understanding the WebLogic Solution....127
Using the WebLogic Solution Template....129

Chapter 12: WebSphere Solution Template....135
Understanding the WebSphere Solution....135
Using the WebSphere Solution Template....137

PART III: SITESCOPE MONITORS

Chapter 13: Apache Server Monitor 143
About the Apache Server Monitor 143
Configuring the Apache Server Monitor 144

Chapter 14: ASP Server Monitor 151
About the ASP Server Monitor 151
Configuring the ASP Server Monitor 152

Chapter 15: BroadVision Application Server Monitor 159
About the BroadVision Application Server Monitor 159
Configuring the BroadVision Application Server Monitor 160

Chapter 16: Check Point Firewall-1 Monitor 167
About the Check Point Firewall-1 Monitor 167
Configuring the Check Point Firewall-1 Monitor 167

Chapter 17: Cisco Works Monitor 175
About the Cisco Works Monitor 175
Configuring the Cisco Works Monitor 175

Chapter 18: Citrix Server Monitor 187
About the Citrix Server Monitor 187
Configuring the Citrix Server Monitor 188
Troubleshooting Tips for the Citrix Server Monitor 195

Chapter 19: Composite Monitor 197
About the Composite Monitor 197
Configuring the Composite Monitor 198

Chapter 20: ColdFusion Server Monitor 205
About the ColdFusion Server Monitor 205
Configuring the ColdFusion Server Monitor 206

Chapter 21: CPU Utilization Monitor 213
About the CPU Utilization Monitor 213
Configuring the CPU Utilization Monitor 214

Chapter 22: Database Counter Monitor 221
About the Database Counter Monitor 221
Editing the Database Counter Monitor 223

Chapter 23: Database Query Monitor 233
About the Database Query Monitor 233
Setup Requirements for the Database Query Monitor 234
Configuring the Database Query Monitor 235

Chapter 24: DB2 Monitor 249
About the DB2 Monitor 249
Configuring the DB2 Monitor 250

Chapter 25: DB2 8.x Monitor 261
About the DB2 8.x Monitor 261
Configuring the DB2 8.x Monitor 262

Chapter 26: Disk Space Monitor 273
About the Disk Space Monitor 273
Configuring the Disk Space Monitor 274

Chapter 27: Directory Monitor 281
About the Directory Monitor 281
Configuring the Directory Monitor 282

Chapter 28: DHCP Monitor 289
About the DHCP Monitor 289
Installation of DHCP Software Library 290
Configuring the DHCP Monitor 290

Chapter 29: DNS Monitor 297
About the DNS Monitor 297
Configuring the DNS Monitor 298

Chapter 30: Dynamo Application Server Monitor 305
About the Dynamo Application Server Monitor 305
Configuring the Dynamo Application Server Monitor 306

Chapter 31: eBusiness Chain Monitor 315
About the eBusiness Chain Monitor 315
Setting up Monitors for the eBusiness Chain 317
Configuring the eBusiness Chain Monitor 318
Passing Values from One Monitor to Another 324

Chapter 32: F5 Big-IP Monitor 325
About the F5 Big-IP Monitor 325
Configuring the F5 Big-IP Monitor 325

Chapter 33: File Monitor 335
About the File Monitor 335
Configuring the File Monitor 336

Chapter 34: Formula Composite Monitor 345
About the Formula Composite Monitor 345
Configuring the Formula Composite Monitor 347

Chapter 35: FTP Monitor....355
About the FTP Monitor....355
Configuring the FTP Monitor....357

Chapter 36: IIS Server Monitor....365
About the IIS Server Monitor....365
Configuring the IIS Server Monitor....366

Chapter 37: iPlanet Server Monitor....373
About the iPlanet Server Monitor....373
Configuring the iPlanet Server Monitor....375

Chapter 38: IPMI Monitor....387
About the IPMI Monitor....387
System Requirements....387
Configuring the IPMI Monitor....388

Chapter 39: JMX Monitor....395
About the JMX Monitor....395
Usage Guidelines....396
Configuring the JMX Monitor....397

Chapter 40: LDAP Monitor....403
About the LDAP Monitor....403
Configuring the LDAP Monitor....404

Chapter 41: Link Check Monitor....413
About the Link Check Monitor....413
Configuring the Link Check Monitor....414

Chapter 42: Log File Monitor....423
About the Log File Monitor....423
Configuring the Log File Monitor....424

Chapter 43: Mail Monitor....435
About the Mail Monitor....435
Configuring the Mail Monitor....436

Chapter 44: MAPI Monitor....445
About the MAPI Monitor....445
System Requirements....445
Configuring the MAPI Monitor....449

Chapter 45: Memory Monitor....455
About the Memory Monitor....455
Configuring the Memory Monitor....457

Chapter 46: Network Bandwidth Monitor 463
About the Network Bandwidth Monitor 463
Configuring the Network Bandwidth Monitor 464

Chapter 47: Network Monitor 477
About the Network Monitor 477
Configuring the Network Monitor 478

Chapter 48: News Monitor 485
About the News Monitor 485
Configuring the News Monitor 486

Chapter 49: Oracle9i Application Server Monitor 493
About the Oracle9i Application Server Monitor 493
Configuring the Oracle9i Application Server Monitor 494

Chapter 50: Oracle Database Monitor 503
About the Oracle Database Monitor 503
Configuring the Oracle Database Monitor 505

Chapter 51: Ping Monitor 513
About the Ping Monitor 513
Configuring the Ping Monitor 514

Chapter 52: Port Monitor 521
About the Port Monitor 521
Configuring the Port Monitor 522

Chapter 53: Radius Monitor 529
About the Radius Monitor 529
Configuring the Radius Monitor 530

Chapter 54: Real Media Player Monitor 537
About the Real Media Player Monitor 537
Configuring the Real Media Player Monitor 538

Chapter 55: Real Media Server Monitor 545
About the Real Media Server Monitor 545
Configuring the Real Media Server Monitor 546

Chapter 56: Real Time Streaming Protocol Monitor 553
About the RTSP Monitor 553
Configuring the RTSP Monitor 557

Chapter 57: SAP Monitor 563
About the SAP Monitor 563
SAP Java Connector Installation 564
Configuring the SAP Monitor 565

Chapter 58: Script Monitor 573
About the Script Monitor 573
Configuring the Script Monitor 576
Setting a Timeout Value for Script Execution 584

Chapter 59: Service Monitor 587
About the Service Monitor 587
Configuring the Service Monitor 588

Chapter 60: SilverStream Server Monitor 595
About the SilverStream Server Monitor 595
Configuring the SilverStream Server Monitor 596

Chapter 61: SNMP Monitor 605
About the SNMP Monitor 605
Configuring the SNMP Monitor 606

Chapter 62: SNMP by MIB Monitor 617
About the SNMP by MIB Monitor 617
Configuring the SNMP by MIB Monitor 618

Chapter 63: SNMP Trap Monitor 629
About the SNMP Trap Monitor 629
Configuring the SNMP Trap Monitor 630

Chapter 64: SQL Server Monitor 637
About the SQL Server Monitor 637
Configuring the SQL Server Monitor 638

Chapter 65: SunONE Server Monitor 645
About the SunONE Server Monitor 645
Configuring the SunONE Server Monitor 646
SunONE Server Counters 653
Browse Counters Utility 656

Chapter 66: Sybase Monitor 659
About the Sybase Monitor 659
Configuring the Sybase Monitor 660

Chapter 67: Tuxedo Monitor 671
About the Tuxedo Monitor 671
Configuring the Tuxedo Monitor 672

Chapter 68: Unix Resources Monitor 681
About the Unix Resources Monitor 681
Configuring the Unix Resources Monitor 682

Chapter 69: URL Monitor 695
About the URL Monitor 695
Configuring the URL Monitor 698

Chapter 70: URL Content Monitor 713
About the URL Content Monitor 713
Configuring the URL Content Monitor 715

Chapter 71: URL List Monitor 725
About the URL List Monitor 725
Configuring the URL List Monitor 727

Chapter 72: URL Sequence Monitor 735
Understanding the URL Sequence Monitor 735
Working with the URL Sequence Monitor 736
Configuring the URL Sequence Monitor 738
Configuring URL Sequence Steps 739
Settings for URL Sequence Steps 746
URL Sequence Monitor Settings 750
Retaining and Passing Values Between Sequence Steps 759

Chapter 73: Web Server Monitor 761
About the Web Server Monitor 761
Configuring the Web Server Monitor 762

Chapter 74: Web Service Monitor 769
About the Web Service Monitor 769
Configuring the Web Service Monitor 771

Chapter 75: WebLogic Application Server Monitor 781
About the WebLogic Application Server Monitor 781
Configuring the WebLogic Application Server Monitor 784

Chapter 76: WebSphere Application Server Monitor 793
About the WebSphere Application Server Monitor 793
System Requirements 793
Configuring the WebSphere Application Server Monitor 798

Chapter 77: WebSphere Performance Servlet Monitor 807
About the WebSphere Performance Servlet Monitor 807
Configuring the WebSphere Performance Servlet Monitor 808

Chapter 78: Windows Services State Monitor 817
About the Windows Services State Monitor 817
Configuring the Windows Services State Monitor 818

Chapter 79: Windows Dial-up Monitor 825
About the Windows Dial-up Monitor 825
Configuring the Windows Dial-up Monitor 827

Chapter 80: Windows Event Log Monitor 835
About the Windows Event Log Monitor 835
Configuring the Windows Event Log Monitor 836

Chapter 81: Windows Performance Counter Monitor 845
About the Windows Performance Counter Monitor 845
Configuring the Windows Performance Counter Monitor 845

Chapter 82: Windows Media Player Monitor 855
About the Windows Media Player Monitor 855
Configuring the Windows Media Player Monitor 856

Chapter 83: Windows Media Server Monitor 863
About the Windows Media Server Monitor 863
Configuring the Windows Media Server Monitor 864

Chapter 84: Windows Resources Monitor 871
About the Windows Resources Monitor 871
Configuring the Windows Resources Monitor 872

Chapter 85: XML Metrics Monitor 881
Working with the XML Metrics Monitor 881
Configuring the XML Metrics Monitor 882

PART IV: OPTIONAL MONITORS

Chapter 86: Active Directory Replication Monitor 895
About the Active Directory Replication Monitor 895
Editing the Active Directory Replication Monitor 896

Chapter 87: COM+ Server Monitor 903
About the COM+ Server Monitor 903
COM+ Probe Installation 904
Configuring the COM+ Server Monitor 905

Chapter 88: Exchange 2003 Mailbox Monitor 913
About the Exchange 2003 Mailbox Monitor 913
Editing the Exchange 2003 Mailbox Monitor 914

Chapter 89: Exchange 2003 Public Folder Monitor 921
About the Exchange 2003 Public Folder Monitor 921
Editing the Exchange 2003 Public Folder Monitor 922

Chapter 90: Exchange 2000/2003 Message Traffic Monitor.....929
About the Exchange 2000/2003 Message Traffic Monitor.....929
Editing the Exchange 2000/2003 Message Traffic Monitor.....930

Chapter 91: Exchange 5.5 Message Traffic Monitor 937
About the Exchange 5.5 Message Traffic Monitor.....937
Editing the Exchange 5.5 Message Traffic Monitor 938

Chapter 92: SAP CCMS Monitor 945
Understanding the SAP CCMS Monitor 945
SAP Java Connector Installation 947
Configuring the SAP CCMS Monitor 949

Chapter 93: SAP CCMS Alerts Monitor.....955
Understanding the SAP CCMS Alerts Monitor 955
SAP Java Connector Installation 957
Configuring the SAP CCMS Alerts Monitor.....958

Chapter 94: SAP Java Web Application Server Monitor.....967
Understanding the SAP Java Web Application Server Monitor.....967
SAP JMX Connector Installation.....968
Configuring the SAP Java Web Application Server Monitor 968

Chapter 95: SAP Work Processes Monitor.....975
Understanding the SAP Work Processes Monitor.....975
SAP Java Connector Installation 977
Configuring the SAP Work Processes Monitor 978

Chapter 96: Siebel Log File Monitor.....985
About the Siebel Log File Monitor 985
Configuring the Siebel Log File Monitor 986

Chapter 97: Siebel Application Server Monitor.....995
About the Siebel Application Server Monitor 995
Configuring the Siebel Application Server Monitor 998

Chapter 98: Siebel Web Server Monitor.....1007
About the Siebel Web Server Monitor.....1007
Configuring the Siebel Web Server Monitor.....1008

Chapter 99: WebSphere MQ Status Monitor 1019
About the WebSphere MQ Status Monitor 1019
Software Prerequisites 1020
List of Available Metrics 1020
Channel Status Codes 1021
Monitoring MQ Events 1022
Authentication 1024
Configuring the WebSphere MQ Status Monitor 1024

Chapter 100: Browsable Windows Performance Counter Monitor 1033
About the Browsable Windows Performance Counter Monitor 1034
Editing the Browsable Windows Performance Counter Monitor 1034

PART V: INTEGRATION MONITORS

Chapter 101: Working with SiteScope Integration Monitors 1043
Integration Monitor Overview 1043
Licensing 1045
Important Upgrade Information 1045
Integration Monitor Logging Options 1046
Troubleshooting Integration Monitors 1047

Chapter 102: Integration Monitor Configuration Files 1049
Introducing Integration Monitor Configuration Files 1049
Understanding Configuration File Structure 1051
Event Handler Structure 1052
Working with Configuration Files 1059

Chapter 103: Avalon Event Monitor 1069
About the Avalon Event Monitor 1069
Setup Requirements 1070
Configuring the Avalon Event Monitor 1071

Chapter 104: BMC PATROL Event Monitor 1079
About the BMC PATROL Event Monitor 1079
Integration Architecture 1082
KM Installation and Configuration 1084
Connectivity Settings 1087
Connectivity Diagnostics 1088
Configuring the BMC PATROL Event Monitor 1089

Chapter 105: BMC PATROL Metrics Monitor 1097
About the BMC PATROL Metrics Monitor 1097
System Requirements 1098
Connectivity Diagnostics 1098
Configuring the BMC PATROL Metrics Monitor 1100

Chapter 106: CA Unicenter Event Monitor 1109
About the CA Unicenter Event Monitor 1109
System Requirements 1110
Configuring the CA Unicenter Event Monitor 1115

Chapter 107: Compaq Insight Manager Event Monitor 1123
About the Compaq Insight Manager Event Monitor 1123
Setup Requirements 1124
Configuring the Compaq Insight Manager Event Monitor 1125

Chapter 108: Concord Metrics Monitor 1135
About the Concord Metrics Monitor 1135
Setup Requirements 1136
Configuring the Concord Metrics Monitor 1137

Chapter 109: HP OVO Event Monitor 1147
About the HP OVO Event Monitor 1147
Integration Architecture 1149
Working with the HP OVO Integration Add-on 1149
Configuring the HP OVO Event Monitor 1153

Chapter 110: HP SIM Event Monitor 1161
About the HP SIM Event Monitor 1161
System Requirements 1162
Configuring the HP SIM Event Monitor 1163

Chapter 111: Mercury Application Mapping Measurement Monitor 1173
About the Mercury Application Mapping Measurement Monitor 1173
Setup Requirements 1174
Configuring the Mercury Application Mapping Measurement Monitor 1175

Chapter 112: Netcool Event Monitor 1185
About the Netcool Event Monitor 1185
Setup Requirements 1186
Configuring the Netcool Event Monitor 1187

Chapter 113: NetIQ Metrics Monitor....1195
About the NetIQ Metrics Monitor....1195
Configuring the NetIQ Metrics Monitor....1197

Chapter 114: Remedy Ticketing Monitor....1207
About Remedy System Terminology....1207
About the Remedy Ticketing Monitor....1208
Software Requirements....1209
Remedy HelpDesk Integration Options for SiteScope....1211
Configuring the Remedy Ticketing Monitor....1214

Chapter 115: Technology Database Integration Monitor....1223
About the Technology Database Integration Monitor....1223
Setup Requirements....1225
Configuring the Technology Database Integration Monitor....1227
Basic Troubleshooting....1240

Chapter 116: Technology Log File Integration Monitor....1243
About the Technology Log File Integration Monitor....1243
Setup Requirements....1244
Configuring the Technology Log File Integration Monitor....1246
Step-by-Step Guide to Integrating Log File Data into Mercury Business Availability Center....1256
Basic Troubleshooting....1259

Chapter 117: Technology SNMP Trap Integration Monitor....1261
About the Technology SNMP Trap Integration Monitor....1261
Setup Requirements....1262
Configuring the Technology SNMP Trap Integration Monitor....1264
Troubleshooting the Technology SNMP Trap Integration Monitor....1274

Chapter 118: Technology Web Service Integration Monitor....1279
About the Technology Web Service Integration Monitor....1279
Setup Requirements....1281
Configuring the Technology Web Service Integration Monitor....1282
Checking Connectivity to the Technology Web Service Integration Monitor....1289

Chapter 119: Tivoli DM Metrics Monitor....1291
About the Tivoli DM Metrics Monitor....1291
Setup Requirements....1292
Configuring the Tivoli DM Metrics Monitor....1293

Chapter 120: Tivoli TEC Event Monitor 1301
About the Tivoli TEC Event Monitor 1301
Integration Architecture 1302
System Requirements 1303
Configuring the Tivoli TEC Event Monitor 1304

Chapter 121: WhatsUp Event Monitor 1313
About the WhatsUp Event Monitor 1313
Configuring the WhatsUp Event Monitor 1314

Chapter 122: Integration with HP Network Node Manager 1325
About Network Node Manager Integration 1325
Writing Scripts to Export Network Node Manager Data 1326
Configuring Events in Network Node Manager 1326

PART VI: MONITOR TROUBLESHOOTING TOOLS

Chapter 123: Tools for Troubleshooting 1331
About SiteScope Tools 1331
Working with SiteScope Tools 1333

Index 1363

Welcome to Configuring SiteScope Monitors

This guide provides instructions on how to configure SiteScope monitors, alerts, reports, and settings.

How This Guide is Organized

The guide contains the following chapters:

Part I Working with Groups, Monitors, and Templates

Describes how to work with groups, introduces how to configure and work with SiteScope monitors, and explains how to work with templates and the Monitor What Matters wizard.

Part II Solution Templates

Describes how to deploy SiteScope monitoring for commonly used IT applications using solution templates.

Part III SiteScope Monitors

Describes how to configure each type of SiteScope standard monitor.

Part IV Optional Monitors

Describes how to configure optional SiteScope monitors and monitor types specific to solution templates.

Part V Integration Monitors

Describes how to configure each type of integration monitors, including the required installation and configuration file procedures, where necessary.

Part VI Monitor Troubleshooting Tools

Describes how to use a number of tools and utilities to help diagnose and troubleshooting issues relating to monitoring with SiteScope.

Who Should Read This Guide

This guide is intended for the following users of Mercury Business Availability Center:

- Mercury Business Availability Center administrators
- Mercury Business Availability Center data collector administrators

Readers of this guide should be knowledgeable about enterprise system administration, infrastructure monitoring systems, and SiteScope, and have familiarity with the systems being set up for monitoring.

Getting More Information

For information on using and updating the Mercury Business Availability Center Documentation Library, reference information on additional documentation resources, typographical conventions used in the Documentation Library, and quick reference information on deploying, administering, and using Mercury Business Availability Center, refer to *Getting Started with Mercury Business Availability Center*.

Part I

Working with Groups, Monitors, and Templates

1

Working with SiteScope Groups

SiteScope groups are containers used to organize SiteScope monitor instances. This section provides an overview of concepts and details for working with SiteScope monitors.

This chapter describes:	On page:
About SiteScope Monitor Groups	3
Working with Monitor Groups	3
Configuring Group Settings	10

About SiteScope Monitor Groups

SiteScope groups are tools for automatically connecting to and querying different kinds of systems and applications used in enterprise business systems.

Monitor instances that you create must be added within a SiteScope monitor group container. Monitor group containers may be nested within other group containers as subgroups. You use group containers to help you organize the monitor instances that you create.

Working with Monitor Groups

The following sections describe the actions that you use with SiteScope groups. This includes a description of the steps you use to add, edit, delete, and perform other actions on groups.

Adding a Group to SiteScope

Groups can be added as a top level element within a SiteScope or as a subgroup within another monitor group container. You should create monitor group containers to make deployment of monitors and associated alerts manageable and effective for your environment and organization.

Groups can be added to SiteScope in more than one way. The simplest way it to add groups individually. Alternatively, you can deploy groups along with multiple monitors by using templates.

Use the following steps to add an group to SiteScope.

Note: The SiteScope must be currently attached to Monitor Administration in order to add a new group to the target SiteScope agent. If the SiteScope is not currently attached, an error message is displayed.

To add a monitor group using the left menu:

1. Using the left menu, select the SiteScope node or existing monitor group container into which you want add the group.
2. Right-click the container in the left menu to display the container action menu and select **New Group**. The New SiteScope Group page is displayed in the Contents panel.
3. Enter a name for the new group in the **Group Name** field.
4. Optionally, expand the Advanced Settings area and enter settings as applicable. See the section "Configuring Group Settings" on page 10 for more details about Advanced Settings for groups.
5. When the required fields are complete, click the **OK** button at the bottom of the properties panel to create the group.

To add a monitor to a group using the container Contents panel:

1. Using the left menu, select the SiteScope node or monitor group container into which you want add the group. The applicable container Contents panel is displayed.

2 Click the **New Group** button new the top of the Contents panel. The New SiteScope Group page is displayed in the Contents panel.

3 Enter a name for the new group in the **Group Name** field.

4 Optionally, expand the Advanced Settings area and enter settings as applicable. See the section "Configuring Group Settings" on page 10 for more details about Advanced Settings for groups.

5 When the required fields are complete, click the **OK** button at the bottom of the properties panel to create the group.

Editing a Group

Note: The SiteScope must be currently attached to Monitor Administration in order to edit a monitor on the target SiteScope agent. If the SiteScope is not currently attached, an error message is displayed.

Use the following steps to edit an existing group:

To edit a group using the left menu:

1 Using the left menu, select the monitor element that you want to edit.

2 Right-click the container in the left menu to display the container action menu and select **Edit**. The monitor properties edit page is displayed in the Contents panel.

3 Edit the monitor properties form as needed. See the help page for the applicable monitor type for information about the property settings.

4 When the required fields are complete, click the **OK** button at the bottom of the properties panel to update the monitor.

To edit a group using the container Contents panel:

1 Using the left menu, select the SiteScope or monitor group element to which you want to add a group. The applicable container Contents panel is displayed.

2 At the top of the Contents panel, click the **New Group** button. The monitor properties edit page is displayed in the Contents panel.

3 Edit the monitor properties form as needed. See the help page for the applicable monitor type for information about the property settings.

4 When the required fields are complete, click the **OK** button at the bottom of the properties panel to update the monitor.

Deleting a Group

Deleting a monitor removes the applicable monitor action from the SiteScope agent. This has the effect of disabling any alert action that was associated with the monitor. As with other actions, there is more than one method that can be used to delete an monitor.

Note: The SiteScope must be currently attached to Monitor Administration in order to delete a monitor from the target SiteScope agent. If the SiteScope is not currently attached, an error message is displayed.

To delete a group using the left menu:

1 Using the left menu, select the monitor element you want to delete.

2 Right-click the container in the left menu to display the container action menu and select **Delete**. A confirmation message is displayed.

3 Click **OK** to confirm the action. The monitor is deleted.

To delete a group using the container Contents panel:

1 Using the left menu, select the container or element to which the monitor is associated. The applicable Contents panel is displayed.

2 In the Monitors section of the Contents panel, check the box corresponding to the monitor (or monitors) you want to delete.

3 Click the **X** button at the bottom of the Monitors section to delete the selected monitor. A confirmation message is displayed.

4 Click **OK** to confirm the action. The monitor is deleted.

Copying a Group

You can copy an existing group and paste it to a new location within the SiteScope tree. Copying a group duplicates the configuration settings for the group and all monitors within the group.

After you copy a group, you will normally need to edit the group and the configuration properties each individual monitor within the group to direct the monitors to a unique system or application. Otherwise, the monitors in the copies group will duplicate the monitoring actions of the original group.

Note: Generally, you should avoid copying groups as it can lead to redundant monitoring and possible group identity problems within SiteScope. You can use templates to more efficiently replicate common group and monitor configuration patterns. See "Using Templates to Deploy Monitors" for more information about working with templates.

Use the following steps to copy a group.

To copy a group using the left menu:

1. Using the left menu, select the monitor group you want to copy.
2. Right-click the container in the left menu to display the container action menu and select **Copy**.
3. Select the SiteScope node or monitor group node where you want the copy of the group to be created.
4. Right-click the container in the left menu to display the container action menu and select **Paste**. SiteScope adds a copy of the group to that selected node.

To edit a group using the container Contents panel:

1. Using the left menu, select the monitor group you want to copy. The applicable container Contents panel is displayed.
2. At the top of the Contents panel, click the **Copy icon** button.

3 Select the SiteScope node or monitor group node where you want the copy of the group to be created. The applicable container Contents panel is displayed.

4 At the top of the Contents panel of the target container, click the **Paste icon** button. SiteScope adds a copy of the group to that selected container node.

Adding an Alert to a Group

You can create a group alert by adding an alert definition to a group container. By default a group alert is associated with all monitors within the group. This means that when any one monitor in the group reports the status category defined for the alert (for example, error or warning), the group alert will be triggered. You can configure a group alert to exclude one or more of the monitors in the group by using the **Alert Targets** selection tree. Use the following steps to add an alert to a group.

To add an alert to a group using the left menu:

1 Using the left menu, select the monitor group container into which you want add the alert.

2 Right-click the container in the left menu to display the container action menu and select **New Alert**. The New Alert selection list is displayed in the Contents panel.

3 Click on the name of the alert type that you want to add. The alert properties page for the applicable monitor type is displayed.

4 Select the monitors that should trigger this alert. Complete the other alert properties as indicated. See the help page for the applicable alert type for information on system requirements and other detailed information about the property settings.

5 When the required fields are complete, click the **OK** button at the bottom of the properties panel to create the alert definition.

To add an alert to a group using the container Contents panel:

1 Using the left menu, select the monitor group container into which you want add the alert. The applicable container Contents panel is displayed.

2 Click the **New Alert** button at the top of the Contents panel. The New Alert selection list is displayed in the Contents panel.

3 Click on the name of the alert type that you want to add. The alert properties page for the applicable monitor type is displayed.

4 Select the monitors that should trigger this alert. Complete the other alert properties as indicated. See the help page for the applicable alert type for information on system requirements and other detailed information about the property settings.

5 When the required fields are complete, click the **OK** button at the bottom of the properties panel to create the alert definition.

Adding a Report to a Group

You can create a group report by adding a report definition to a group container. By default a group report includes data from all monitors within the group. You can configure a group report to exclude one or more of the monitors in the group by using the **Monitors and Groups to Report on** selection tree. Use the following steps to add an report to a group.

To add a report to a group using the left menu:

1 Using the left menu, select the monitor group container into which you want add the report.

2 Right-click the container in the left menu to display the container action menu and select **New Report**. The New SiteScope Report selection list is displayed in the Contents panel.

3 Click on the name of the report type that you want to add. The report properties page for the applicable monitor type is displayed.

4 Select the monitors whose data should be included in this report. Complete the other report properties as indicated. See the help page for the applicable report type for information about the property settings.

5 When the required fields are complete, click the **OK** button at the bottom of the properties panel to create the report definition.

To add a report to a group using the container Contents panel:

1 Using the left menu, select the monitor group container into which you want add the report. The applicable container Contents panel is displayed.

2 Click the **New Report** button at the top of the Contents panel. The New SiteScope Report selection list is displayed in the Contents panel.

3. Click on the name of the report type that you want to add. The report properties page for the applicable monitor type is displayed.
4. Select the monitors whose data should be included in this report. Complete the other report properties as indicated. See the help page for the applicable report type for information about the property settings.
5. When the required fields are complete, click the **OK** button at the bottom of the properties panel to create the report definition.

Configuring Group Settings

All SiteScope monitor types have several settings that are common to all monitors or common to a group of monitor types. This section describes these settings and how to configure them.

Main Settings for Groups

You use the Main Settings section to specify how SiteScope should connect to or check the target system. This will vary based on the monitor type. See the section for that particular monitor type for more information. You also select how often the monitor instance should be run and the text name used for this monitor instance in the this product context interface. The following describes the common Main Setting settings:

Group Name

This is a text display name for the monitor group. This text is displayed in the Monitor Administration interface. Choose a name that meaningfully describes the content of the group or the purpose the monitors added to the group will server. For example, you may want to choose a name that represents the element or system that is being monitored. Since you will normally have many monitor groups, you should also use a useful naming convention for all groups. This will make creating view filters and category assignments more effective. For example, you can use a naming convention of *hostname* or *business_unit resource_name* or *resource_type*.

Advanced Settings for Groups

The Advanced Settings section presents settings you can use to customize the behavior of all monitors added to the group and the group information displayed in the product interface. The following describes the Advanced Settings for groups.

Group Refresh Frequency

A group can be assigned a refresh schedule to synchronize the running of all the monitors in that group. Once the Group Refresh Frequency is defined, all the monitors in that group will stop running according to their own schedule (the Frequency setting for the monitor instance), and only run by the Group Refresh Frequency. Other properties of the monitor will continue to function as before. For example, if an individual monitor within the group is disabled, it will remain disabled when the group is scheduled to run.

Note: Group Refresh Frequencies are not applied to sub groups that may be contained by the group.

Once the Group Refresh Frequency is set to 0, it will stop functioning, and the monitors schedule will take control. Once a group schedule is set, any operation on the group (e.g. adding a new monitor, refreshing a monitor, updating a monitor) will cause a refresh on all the group.

To set a refresh frequency for a group:

1. Using the left menu, select the group container element that you want to edit.
2. Right-click the container in the left menu to display the container action menu and select **Edit**. The group properties edit page is displayed in the Contents panel.
3. Expand the Advanced Settings area. Enter a time value in the first text box to the right of the **Group Refresh Frequency** label. Use the drop-down list to select a time increment for the Group Refresh Frequency.

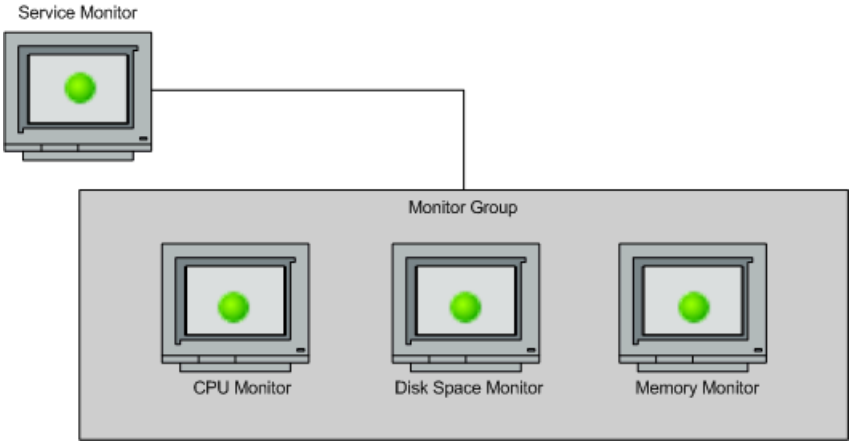
Note: The value for the Group Refresh Frequency must be set to a time value of at least 60 seconds or more. If it is set to a value less than 60 seconds, the Group Refresh Frequency will not be activated.

---

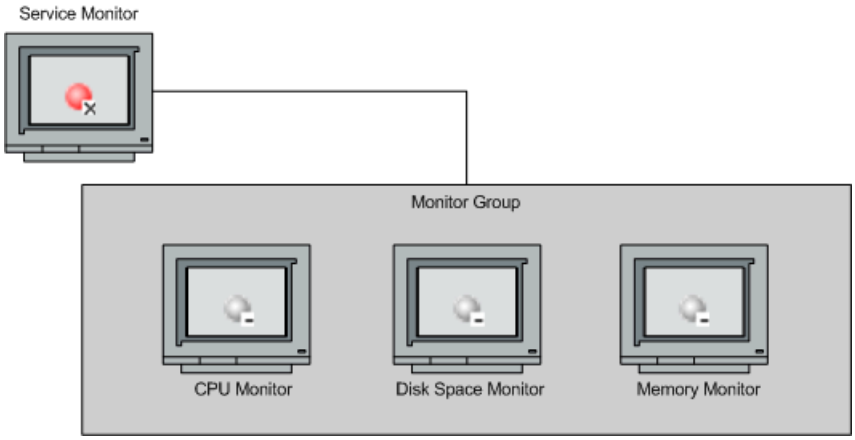
4 Click **OK** to save the changes.

Depends On

You use this option to make the running of this monitor dependent on the status of another monitor or monitor group. This can be used to prevent redundant alerting from multiple monitors that are monitoring different aspects of a single system. You can create a simple system monitor to check the basic availability or "heartbeat" of a system and then create other monitors that perform more detailed tests of that system. The figure below shows an example dependency relationship where three system monitors have been made dependent on a Service Monitor instance.



The detailed test monitors can be made dependent on the status of the "heartbeat" monitor by selecting that monitor. This means the dependent monitors will run as long as the dependency condition is satisfied. If the "heartbeat" monitor detects that the target system has become unavailable, the dependency relationship will automatically disable the other monitors. This has the effect of disabling any alerts that would have been generated by those monitors. The figure below shows the example monitors are disabled because the monitors upon which they depend is reporting an error condition.



By default, no dependency is set for a monitor instance. Use the drop-down list to select the monitor on which this monitor is dependent. Select None to remove any dependency.

Depends Condition

If you choose to make a monitor dependent on the status of another monitor (by using the **Depends On** setting), you use this option to select the status category or condition that the **Depends On** monitor should have for the current monitor to run normally. The monitor being configured will be run normally as long as the monitor selected in the **Depends On** field reports the condition selected in this field. For example, by selecting OK, this monitor is only enabled as long as the monitor selected in the **Depends On** field reports a status of good or OK. The current monitor will automatically be disabled if the monitor selected in the **Depends On** field reports a category or condition other than the condition selected for this setting. See the examples for the Depends On setting.

Group Description

You use this field to enter additional information to describe a group. The **Group Description** can include HTML tags such as the <BR>, <HR>, and <B> tags to control display format and style. The description text will appear on the Content panel for the SiteScope installation.

Category Settings

The Category settings are used to filter items in the SiteScope views. For more information see "Working with Categories" in *Working with Monitor Administration*.

2

Working with SiteScope Monitors

SiteScope monitors are individually configured instruction sets that automatically test systems and services in the network environment. The tests that are performed depend on the type of monitor. SiteScope includes monitors that can test system availability at several levels. This section provides an overview of concepts and details for working with SiteScope monitors.

This chapter describes:	On page:
About SiteScope Monitors	15
SiteScope Monitor Types	16
Monitoring Remote Servers	19
Common Monitor Actions	25
Common Monitor Settings	31

About SiteScope Monitors

SiteScope monitors are tools for automatically connecting to and querying different kinds of systems and applications used in enterprise business systems. The different monitor types provide the generic capabilities for performing actions specific to different systems. You create one or more instances of a monitor type to instruct SiteScope how to monitor specific elements in your IT infrastructure.

One way of thinking about SiteScope monitors is that a monitor instance is an individual group of settings used to control the action of a particular SiteScope monitor type. For example, you can create 100 monitor instances that instruct the SiteScope CPU Monitor type to connect to and measure CPU utilization on remote servers. Each monitor instance contains a different setting defining which remote server is to be monitored and how often. SiteScope is then configured to automatically monitor the CPU utilization on 100 servers at regular intervals.

Monitor instances that you create must be added within a SiteScope monitor group container. Monitor group containers may be nested within other group containers as subgroups. You use group containers to help you organize the monitor instances that you create.

SiteScope Monitor Types

SiteScope monitor types are grouped according to classes that indicates their availability and category that reflect their function. When you select to add a new monitor to a SiteScope agent, the list of available monitor types for that agent are displayed both alphabetically and divided by category in the product interface. The availability of the monitor type is dependent on the class of monitor. This section describes the monitor classes and the category listing formats.

Classes of SiteScope Monitors

The following describes the classes of SiteScope monitors based on licensing requirements. The monitor class controls how the monitor can be accessed and deployed. It also controls where and when it is displayed in the product interface.

Solution Template Monitors

Solution template monitor types are a special class of monitors that enable new monitoring capabilities for specific applications and environments. As part of a solution template, these monitor types are deployed automatically together with other, standard monitor types to provide a monitoring solution that incorporates best practice configurations. These monitor types are controlled by option licensing and can only be added by deploying the applicable solution template. Once they have been deployed, you can edit or delete them using the same steps as with other monitor types. See the section "Introducing SiteScope Solution Templates" for more information.

The monitor types are only available using solution templates include:

- Active Directory Replication Monitor
- Database Counter Monitor
- Exchange 2003 Mailbox Monitor
- Exchange 2000/2003 Message Traffic Monitor
- Exchange 2003 Public Folder Monitor
- Exchange 5.5 Message Traffic Monitor
- Browsable Windows Performance Counter Monitor

Standard Monitors

Standard monitor types represent the monitor types available with a general SiteScope license. These monitor types include many of the general purpose monitor types. See the section for the particular monitor type for information on the usage and configuring each monitor type.

Optional Monitors

New monitoring capabilities are regularly added in SiteScope to support the changing customer needs. There are a number of optional monitor types that add specialized capabilities for monitoring specific applications and servers. These optional monitor types require additional licensing and setup. The sections that describe these monitor types are included with the other standard monitor types in alphabetically order. Contact your Mercury sales for more information about licensing for optional monitors.

Optional Monitors include the following monitor types:

- COM+ Server Monitor
- SAP CCMS Monitor
- Siebel Log File Monitor
- Siebel Application Server Monitor
- Siebel Web Server Monitor
- WebSphere MQ Status Monitor

Integration Monitors

This group of optional monitor types are used to integrate Mercury Interactive products with other commonly used Enterprise Management systems and applications. They are presented in a separate section on the New SiteScope Monitor panel.

These monitor types require additional licensing and may only be available as part of another Mercury product. For more information about Integration Monitor capabilities, see the section on "Working with SiteScope Integration Monitors" on page 1043.

Categories of Monitors

The following describes the SiteScope monitor categories used for the SiteScope Monitors by Category listing. These categories are a guide to the type of infrastructure systems and resources that can be monitored.

Network Services Monitors

Monitors that test commonly used network applications and services by simulating end user actions. These include accessing Web content, e-mail, file downloads, and performing database queries. This subcategory also includes monitors for checking lower level network function and connectivity.

Server Monitors

Monitors that measure server availability, resource usage, and other operating system attributes. These can be used to monitor remote servers running Windows or UNIX-based operating systems.

Application Monitors

Monitors designed to check the availability and report on performance statistics of specific network applications and servers. Most monitors in this category allow you to set monitor status thresholds on more than one measurement per monitor instance. Several of these monitors are specific to Microsoft Windows environments. Many require special setup procedures.

Advanced Monitors

Monitors that provide specific functionality for less commonly used protocols, services, or special adaptations.

Monitoring Remote Servers

Some SiteScope monitors use Internet protocols to test Web systems and applications. Other SiteScope monitors (CPU, Disk Space, Memory, Service and Web Server) use the network file system services and commands to monitor information on remote servers. This includes servers running the following operating systems:

- Windows NT/2000
- Sun Solaris
- SGI Irix
- HP/UX
- Linux

Note: Monitors that can be used to monitor remote servers directly through the network file system are limited to the CPU, Disk Space, Memory, Service, Script (UNIX Only), NT Performance Counter, NT Event Log, or Web Server (Windows Only) monitors.

Note: Monitoring remote Windows servers requires SiteScope for Windows NT/2000 and that the SiteScope service runs in a user or administrative account that has permission to access the Windows Performance registry on the remote servers to be monitored. For Windows NT/2000 servers, use the Services control panel to make changes to the user account used by the SiteScope service. Select the SiteScope service from the list of services, click the Startup button, and fill in the **Log On As** fields with an account that can access the remote servers. Stop and start the SiteScope service to start using the new account.

To monitor certain server level parameters on a remote server using the network files system services, you need to create a remote server profile. A table of server profiles is listed on the UNIX Servers or Windows Servers pages. You access these pages via the Preferences menu. The remote server profiles contain the address and connection information that SiteScope needs to make a remote connection.

After creating remote server profiles, set up monitors to use the remote connection profile. For more information about remotely monitoring either UNIX or NT servers, see the sections on "UNIX Remote Preferences" and "Windows Remote Preferences" in *Managing SiteScope*.

The requirements for monitoring services and applications that are running on remote servers will vary according to the application and network policies in your environment. See the section "Overview of Ports Used for SiteScope Monitoring" below for more information about how many of the SiteScope monitors connect to remote systems. You can also check the on-line Knowledge Base available via the Customer Support site for other information relating to monitoring remote servers.

Overview of Ports Used for SiteScope Monitoring

The following table lists the network ports that are generally used for SiteScope monitoring. In many cases, alternate ports may be configured depending on the security requirements of your environment.

Monitor Type	Ports Used
Apache Server Monitor	Port which Apache Server Admin pages located. Configurable via server configuration file.
ASP Server	Windows Performance Counters over ports 137, 138, and 139 (NetBIOS).
BroadVision App Server	Uses the Object Request Broker (ORB) port number for the BroadVision server you are trying to monitor.
Checkpoint Firewall -1	SNMP monitor. Default is port 161.This is configurable.
Cisco Works	Cisco Works resources are usually available via port 161 or 162 (SNMP), depending on the configuration of the server.
Citrix Server	Ports 137, 138, and 139 (NetBIOS).
ColdFusion Server	Ports 137, 138, and 139 (NetBIOS).
CPU Utilization	For local CPU, no ports required. For CPU's on remote servers: ports 137, 138, and 139 (NetBIOS) for Windows based systems, ports 22 (SSH), 23 (telnet), or 513 (rlogin) for UNIX/Linux based systems<.
Database Query	This is configurable and depends on ODBC or JDBC driver and DB configuration.
DB2	Default is port 50000. This is configurable.
DHCP	Default is port 68.
Directory	For local directories, no ports required. For directories on remote servers: ports 137, 138, and 139 (NetBIOS) for Windows based systems, ports 22 (SSH), 23 (telnet), or 513 (rlogin) for UNIX/Linux based systems.

Disk Space	For the local disk, no ports required. For disks on remote servers: ports 137, 138, and 139 (NetBIOS) for Windows based systems, ports 22 (SSH), 23 (telnet), or 513 (rlogin) for UNIX/Linux based systems.
DNS	Default is port 53.
Dynamo Application	Uses SNMP. This is configurable.
F5 Big IP	Uses SNMP. This is configurable.
File	Local disk. No ports required. For files on remote servers: ports 137, 138, and 139 (NetBIOS). for Windows based systems, ports 22 (SSH), 23 (telnet), or 513 (rlogin) for UNIX/Linux based systems.
FTP	Default is port 21.This is configurable.
IIS Server	Windows Performance Counters over ports 137, 138, and 139 (NetBIOS).
iPlanet Server	Configurable via the iPlanet server administration page.
LDAP	The default is port 389. This is configurable.
Link Check	The default is port 80. This is configurable.
Log File	Ports 137, 138, and 139 (NetBIOS) for Windows based systems, ports 22 (SSH), 23 (telnet), or 513 (rlogin) for UNIX/Linux based systems.
Mail	Port 110 for POP3, port 25 for SMTP, port 143 for IMAP.
MAPI	MAPI uses the Name Service Provider Interface (NSPI) on a dynamically assigned port higher than 1024 to perform client-directory lookup.
Memory	Ports 137, 138, and 139 (NetBIOS) for Windows based systems, ports 22 (SSH), 23 (telnet), or 513 (rlogin) for UNIX/Linux based systems.
Network	No ports required; monitors only the local machine.
News	Default is port 144. This is configurable.

NT Event Log	Ports 137, 138, and 139 (NetBIOS).
Windows Performance Counter	Ports 137, 138, and 139 (NetBIOS).
Oracle Database (JDBC)	This is configurable. Depends on target DB. Default is port 1521.
Oracle9i App Server	This is configurable. Port which Webcaching admin page located.
Ping	Default is port 7.
Port	Monitors any port.
Radius	Currently supports Password Authentication Procedure (PAP) authentication but not the Challenge Handshake Authentication Protocol (CHAP) or Microsoft Challenge Handshake Authentication Protocol (MS-CHAP). The RADIUS servers must be configured to accept PAP requests. Default is port 1645. In recent changes to the RADIUS spec, this may be changed to 1812. The monitor is configurable.
Real Media Player	Uses Real Media client on Sitescope box. Uses the port from which the media content is streamed (based on the URL).
Real Media Server	Ports 137, 138, and 139 (NetBIOS).
RTSP	Uses the port from which the media content is streamed.
SAP	Uses SAP Client software (SAP Front End) to execute certain SAP transactions. Therefore, same ports as SAP.
Script	Ports 137, 138, and 139 (NetBIOS) for Windows based systems, ports 22 (SSH), 23 (telnet), or 513 (rlogin) for UNIX/Linux based systems.
Service	Ports 137, 138, and 139 (NetBIOS) for Windows based systems, ports 22 (SSH), 23 (telnet), or 513 (rlogin) for UNIX/Linux based systems.

SilverStream	Configurable URL (Port number included in URL) to the applicable SilverStream server administration web page.
SNMP	Default is port 161. This is configurable.
SNMP Trap	Uses port 162 for receiving traps.
SQL Server	Ports 137, 138, and 139 (NetBIOS).
SunOne Webserver	URL to the stats-xml file on the target SunONE server. The port is configurable.
Sybase	Monitor requires "Sybase Central" client on the machine where SiteScope is running in order to connect to the Adaptive Server Enterprise Monitor Server. Port number the same as Sybase client.
Tuxedo	The default port for the TUXEDO workstation listener is port 65535. This is configurable.
URL	Generally port number 80. This is configurable.
Web Server	Ports 137, 138, and 139 (NetBIOS) for Windows based systems, ports 22 (SSH), 23 (telnet), or 513 (rlogin) for UNIX/Linux based systems.
Web Service	This is configurable.
WebLogic App Server	BEA WebLogic Application Server monitor uses the Java JMX interface. Port is configurable.
WebSphere App Server	Same port as the IBM WebSphere Administrator's Console.
WebSphere Performance Servlet	WebSphere Performance Servlet. Port is configurable.
Windows Media Player	Same port as media content to be monitored.
Windows Media Server	Ports 137, 138, and 139 (NetBIOS).

Common Monitor Actions

The following sections describe the actions that are common to SiteScope monitors. This includes a description of the steps you use to add, edit, delete, and perform other actions on monitors.

Adding a Monitor to a Group

Monitors must be added to a monitor group container within a SiteScope container for the SiteScope agent that will execute the monitor action. You should create monitor group containers to make deployment of monitors and associated alerts manageable and effective for your environment and organization.

Use the following steps to add an individual monitor to a SiteScope group.

Note: The SiteScope must be currently attached to Monitor Administration in order to add a new monitor to the target SiteScope agent. If the SiteScope is not currently attached, an error message is displayed.

To add a monitor to a group using the left menu:

1. Using the left menu, select the monitor group container into which you want add the monitor.
2. Right-click the container in the left menu to display the container action menu and select **New Monitor**. The New SiteScope Monitor selection list is displayed in the Contents panel.
3. Click on the monitor name for the monitor type that you want to add. You may use the SiteScope Monitors Listed Alphabetically panel or the SiteScope Monitors Listed by Category panel. The new monitor properties page for the applicable monitor type is displayed.
4. Complete the monitor properties form as indicated. See the help page for the applicable monitor type for information on system requirements, applications, and other detailed information about the property settings.
5. When the required fields are complete, click the **OK** button at the bottom of the properties panel to create the monitor.

To add a monitor to a group using the container Contents panel:

1. Using the left menu, select the monitor group container into which you want add the monitor. The applicable container Contents panel is displayed.
2. Click the New Monitor button new the top of the Contents panel. The New SiteScope Monitor selection list is displayed in the Contents panel.
3. Click on the monitor name for the monitor type that you want to add. You may use the SiteScope Monitors Listed Alphabetically panel or the SiteScope Monitors Listed by Category panel. The new monitor properties page for the applicable monitor type is displayed.
4. Complete the monitor properties form as indicated. See the help page for the applicable monitor type for information on system requirements, applications, and other detailed information about the property settings.
5. When the required fields are complete, click the **OK** button at the bottom of the properties panel to create the monitor.

Editing a Monitor

Note: The SiteScope must be currently attached to Monitor Administration in order to edit a monitor on the target SiteScope agent. If the SiteScope is not currently attached, an error message is displayed.

Use the following steps to edit an existing monitor.

To edit a monitor to a group using the monitor tree menu:

1. Using the monitor tree, select the monitor element that you want to edit.
2. Right-click the container in the monitor tree to display the container action menu and select **Edit**. The monitor properties edit page is displayed in the Contents panel.
3. Edit the monitor properties form as needed. See the help page for the applicable monitor type for information about the property settings.
4. When the required fields are complete, click the **OK** button at the bottom of the properties panel to update the monitor.

To edit a monitor to a group using the container Contents panel:

1. Using the left menu, select the monitor element that you want to edit. The applicable container Contents panel is displayed.
2. In the Monitors section, click on the monitor edit icon to the right of the monitor that you want to edit. The monitor properties edit page is displayed in the Contents panel.
3. Edit the monitor properties form as needed. See the help page for the applicable monitor type for information about the property settings.
4. When the required fields are complete, click the **OK** button at the bottom of the properties panel to update the monitor.

Deleting a Monitor

Deleting a monitor removes the applicable monitor action from the SiteScope agent. This has the effect of disabling any alert action that was associated with the monitor. As with other actions, there is more than one method that can be used to delete an monitor.

Note: The SiteScope must be currently attached to Monitor Administration in order to delete a monitor from the target SiteScope agent. If the SiteScope is not currently attached, an error message is displayed.

To delete a monitor using the left menu:

1. Using the left menu, select the monitor element you want to delete.
2. Right-click the container in the left menu to display the container action menu and select **Delete**. A confirmation message is displayed.
3. Click **OK** to confirm the action. The monitor is deleted.

To delete an monitor using the container Contents panel:

1. Using the left menu, select the container or element to which the monitor is associated. The applicable Contents panel is displayed.
2. In the Monitors section of the Contents panel, check the box corresponding to the monitor (or monitors) you want to delete.

3 Click the **X** button at the bottom of the Monitors section to delete the selected monitor. A confirmation message is displayed.

4 Click **OK** to confirm the action. The monitor is deleted.

Copying a Monitor

You can copy an existing monitor and paste the copy into any monitor group in the SiteScope tree. Copying a monitor duplicates the configuration settings for the monitor.

After you copy a monitor, you will normally need to edit the monitor to change the system or application that the monitor is targeting. Otherwise, the copied monitors will duplicate the monitoring actions of the original monitor.

Use the following steps to copy a monitor.

To copy a monitor using the left menu:

1 Using the left menu, select the monitor you want to copy.

2 Right-click the container in the left menu to display the container action menu and select **Copy**.

3 Select the monitor group node where you want the copy of the monitor to be created.

4 Right-click the container in the left menu to display the container action menu and select **Paste**. SiteScope adds a copy of the monitor to the selected monitor group.

To edit a monitor using the container Contents panel:

1 Using the left menu, select the monitor you want to copy. The applicable container Contents panel is displayed.

2 At the top of the Contents panel, click the **Copy icon** button.

3 Select the monitor group node where you want the copy of the monitor to be created. The applicable container Contents panel is displayed.

4 At the top of the Contents panel of the target container, click the **Paste icon** button. SiteScope adds a copy of the monitor to the selected monitor group.

Adding an Alert to a Group

You can create an alert for an individual monitor by adding an alert definition to a monitor container. Use the following steps to add an alert to a monitor.

To add an alert to a monitor using the left menu:

1. Using the left menu, select the monitor to which you want add the alert.
2. Right-click the container in the left menu to display the container action menu and select **New Alert**. The New Alert selection list is displayed in the Contents panel.
3. Click on the name of the alert type that you want to add. The alert properties page for the applicable monitor type is displayed.
4. Select the monitors that should trigger this alert. Complete the other alert properties as indicated. See the help page for the applicable alert type for information on system requirements and other detailed information about the property settings.
5. When the required fields are complete, click the **OK** button at the bottom of the properties panel to create the alert definition.

To add an alert to a monitor using the container Contents panel:

1. Using the left menu, select the monitor to which you want add the alert. The applicable container Contents panel is displayed.
2. Click the **New Alert** button at the top of the Contents panel. The New Alert selection list is displayed in the Contents panel.
3. Click on the name of the alert type that you want to add. The alert properties page for the applicable monitor type is displayed.
4. Select the monitors that should trigger this alert. Complete the other alert properties as indicated. See the help page for the applicable alert type for information on system requirements and other detailed information about the property settings.
5. When the required fields are complete, click the **OK** button at the bottom of the properties panel to create the alert definition.

Adding a Report to a Monitor

You can create an individual monitor report by adding a report definition to a monitor container. Use the following steps to add an report to a monitor.

To add a report to a monitor using the left menu:

1. Using the left menu, select the monitor to which you want add the report.
2. Right-click the container in the left menu to display the container action menu and select **New Report**. The New SiteScope Report selection list is displayed in the Contents panel.
3. Click on the name of the report type that you want to add. The report properties page for the applicable monitor type is displayed.
4. Select the monitors whose data should be included in this report. Complete the other report properties as indicated. See the help page for the applicable report type for information about the property settings.
5. When the required fields are complete, click the **OK** button at the bottom of the properties panel to create the report definition.

To add a report to a monitor using the container Contents panel:

1. Using the left menu, select the monitor to which you want add the report. The applicable container Contents panel is displayed.
2. Click the **New Report** button at the top of the Contents panel. The New SiteScope Report selection list is displayed in the Contents panel.
3. Click on the name of the report type that you want to add. The report properties page for the applicable monitor type is displayed.
4. Select the monitors whose data should be included in this report. Complete the other report properties as indicated. See the help page for the applicable report type for information about the property settings.
5. When the required fields are complete, click the **OK** button at the bottom of the properties panel to create the report definition.

Common Monitor Settings

All SiteScope monitor types have several settings that are common to all monitors or common to a group of monitor types. This section describes these settings and how to configure them.

Common Main Settings

You use the Main Settings section to specify how SiteScope should connect to or check the target system. This will vary based on the monitor type. See the section for that particular monitor type for more information. You also select how often the monitor instance should be run and the text name used for this monitor instance in the this product context interface. The following describes the common Main Setting settings:

Name

This is a text display name for the monitor instance. This text is displayed in the Monitor Administration interface. Choose a name that meaningfully describes the element or system that is being monitored. You should also use a useful naming convention for all monitors. This will make creating view filters and category assignments more effective. For example, you can use a convention of *hostname : resource_type* or *business_unit resource_name monitored_element*. If you do not enter a name text, SiteScope will create a default name based on the host, system, URL being monitored or the default name defined for the monitor type.

Frequency

You use the **Frequency** setting to set how often the monitor should run. This represents how often SiteScope will attempt to execute the action defined for that monitor instance. The status of the monitor will be updated to show the results of each run. The default frequency interval is to run the monitor once every 10 minutes. Use the drop-down list to the right of the text box to specify an update interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Note: Monitor run frequency is an important factor in overall SiteScope monitor load. In environments with many SiteScope monitors configured and run at frequent intervals, monitor load can impact the effectiveness and performance of the SiteScope application, the monitored systems and applications, and network traffic. If you see evidence of these problems, you should review your monitor configurations and associated logs to reduce the run frequency of some monitors.

Common Advanced Settings

The Advanced Settings section presents a number of ways to customize the behavior of a monitor and its display in the product interface. You use this section to set monitor-to-monitor dependencies, customize display options, and configure other settings specific to the particular monitor type that may be required in some infrastructure environments. The following describes the common settings.

Run Monitor On Update

Select this option to have the subject monitor run whenever a change is made to the monitor configuration. The default is to update the monitor configuration without running the monitor action at the time of the update. This reduces load on the SiteScope server which normally would run the monitor whenever a change is made to the configuration. This also can be used to eliminate extra data entries in reports when a change is made to the monitor configuration or someone views a monitor configuration and clicks the **OK** button, even though no changes were made to the monitor configuration.

Note: This option is only available in the new SiteScope interface.

Verify Error

Check this box if you want SiteScope to automatically run the monitor again if it detects an error. When an error is detected, the monitor will immediately be scheduled to run again once. It is recommended that you not use this option as it can cause a number of problems (see the notes below) in large monitoring environments.

Note: In order to change the run frequency of a monitor when an error is detected, you should use the **Error Frequency** option below instead of the **Verify Error** option.

Note: The status returned by the **Verify Error** run of the monitor will replace the status of the originally scheduled run that detected an error. This may cause the loss of important performance data if the data from the verify run is different than the initial error status.

Use of this option across many monitor instances may result in significant monitoring delays in the case that multiple monitors are rescheduled to verify errors at the same time.

Error Frequency

You use this option to set a new monitoring interval for monitors that have reported an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected. The monitor reverts to the run interval specified in the **Frequency** setting when the monitor reports that the status has changed from error to a non-error state.

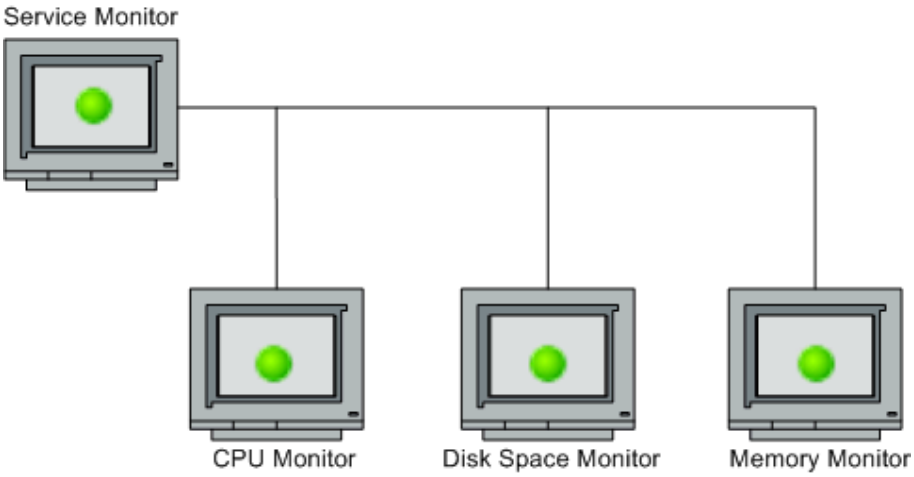
Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

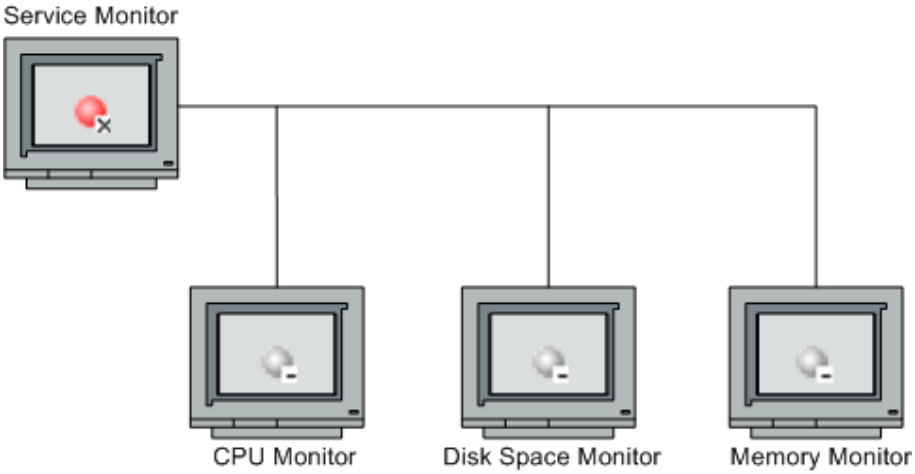
By default, SiteScope monitors are enabled every day of the week. You may, however, schedule your monitors to run only on certain days or on a fixed schedule. This option includes a drop-down selection box that lists the available schedule profiles. For more information about creating monitor schedules, see the section on "Range Schedule Preferences" in *Managing SiteScope* for more information.

Depends On

You use this option to make the running of this monitor dependent on the status of another monitor or monitor group. This can be used to prevent redundant alerting from multiple monitors that are monitoring different aspects of a single system. You can create a simple system monitor to check the basic availability or "heartbeat" of a system and then create other monitors that perform more detailed tests of that system. The figure below shows an example dependency relationship where three system monitors have been made dependent on a Service Monitor instance.



The detailed test monitors can be made dependent on the status of the "heartbeat" monitor by selecting that monitor. This means the dependent monitors will run as long as the dependency condition is satisfied. If the "heartbeat" monitor detects that the target system has become unavailable, the dependency relationship will automatically disable the other monitors. This has the effect of disabling any alerts that would have been generated by those monitors. The figure below shows the example monitors are disabled because the monitors upon which they depend is reporting an error condition.



By default, no dependency is set for a monitor instance. To make the running of the monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make a monitor dependent on the status of another monitor (by using the **Depends On** setting), you use this option to select the status category or condition that the **Depends On** monitor should have for the current monitor to run normally. The monitor being configured will be run normally as long as the monitor selected in the **Depends On** field reports the condition selected in this field. For example, by selecting OK, this monitor is only enabled as long as the monitor selected in the **Depends On** field reports a status of good or OK. The current monitor will automatically be disabled if the monitor selected in the **Depends On** field reports a category or condition other than the condition selected for this setting. See the examples for the Depends On setting.

Monitor Description

You use this field to enter additional information to describe a monitor. The **Monitor Description** can include HTML tags such as the <BR>, <HR>, and <B> tags to control display format and style. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

You use this text box to enter an optional description for this monitor that will make it easier to understand what the monitor does. For example, network traffic or main server response time. This description will be displayed on each bar chart and graph in Management Reports. In the old SiteScope interface, this text string is appended to the tool-tip displayed when you pass the mouse cursor over the status icon for this monitor on the Monitor Detail page.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

Enable Monitor

This is the default setting for monitors. If the monitor has previously been disabled, click this radio button to enable the monitor.

Disable Monitor Indefinitely

Click this option to disable the monitor indefinitely. When a monitor has been disabled, SiteScope continues to schedule the monitor to run based on the **Frequency** setting for the monitor but the monitor action is not executed. SiteScope records a monitor data log entry for the monitor when it was scheduled to be run but reports the monitor status as disabled in the place of measurement data. You click the **Enable Monitor** radio button to enable the monitor.

Note: Disabling monitors indefinitely can seriously impact the effectiveness of system availability monitoring in large monitoring environments. Disabled monitors within monitor subgroups may be overlooked or "forgotten" as their status may not be easily visible unless the subgroup is viewed regularly or a filter is applied to display disabled monitors. You should consider using monitor dependencies, schedule profiles, or one of the time limited options if you find the need to disable one or more monitors.

Disable Monitor for the Next Time Period

Use this option to immediately disable the monitor for a specified period of time. Enter a time period that the monitors should remain disabled. Select minutes, hours or days to define the disable time period as applicable.

Disable Monitor on a One Time Schedule

You use this option to temporarily disable the monitor for a time period in the future. The time period can span more than one day. Enter the time for the start time and an end time using the format hh:mm. Enter the dates for the disable time period using the mm/dd/yy format.

Disable Description

Enter an optional descriptive text in the Disable Description text box. This description will appear as part of the monitor status in the monitor group display. The disable status text will also include a string indicating which disable option is in force for the monitor. For example, the text disabled manually indicates that the monitor was disabled using the **Disable Monitor indefinitely** option.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors.

If no alerts have been associated with the monitor instance, the group, or globally, a message will be displayed in the panel. If one or more alerts are defined for the monitor, an expandable tree fragment is displayed that lists all of the alerts that are associated with the monitor relative to the hierarchy element to which the alert is assigned. For example, if an alert is assigned only to the individual monitor, only the monitor and the alert will be displayed in the tree. If a global SiteScope alert is defined as well as an alert for the group to which the monitor belongs is defined, then the tree will display the SiteScope node and the group node together with the alert nodes for those elements.

The Enable/Disable Alerts options in this section are:

Enable All Associated Alerts

This is the default setting for alerts. If the alerts for the monitor have previously been disabled, click this radio button to enable the alerts.

Disable All Associated Alerts for the Next Time Period

Use this option to immediately disable the alerts for the monitor for a specified period of time. Enter a time period that the alerts should remain disabled. Select minutes, hours or days to define the disable time period as applicable.

Disable All Associated Alerts on a One Time Schedule

You use this option to temporarily disable the alerts for a monitor for a time period in the future. The time period can span more than one day. Enter the time for the start time and an end time using the format hh:mm. Enter the dates for the disable time period using the mm/dd/yy format.

Disable Description

Enter an optional descriptive text in the Disable Description text box.

Threshold Settings

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system.

Status threshold criteria for each monitor instance can be set for three status conditions. These are:

- **Error if**
- **Warning if**
- **Good if**

You can set up one or more status thresholds criteria for each status condition per monitor instance. This is to say that a single monitor instance may have one or more criteria used to determine an error status, one or more conditions to determine a warning status, and one or more conditions to indicate a "good" status. Most monitor types include one default setting for each of the three status conditions. By default, only one threshold is displayed when you first configure the monitor.

While the monitor is enabled, it is assigned a status of good, warning, or error based on results returned by the most recent execution of the monitor action. The measurement taken or the results reported by the monitor are tested against all of the status threshold settings to determine the status that will be reported for the monitor.

The individual threshold criteria results are combined as logical **OR** relationships when more than one threshold condition is defined for any of the three settings. When one or more of the conditions (for example when two conditions for **Error if** setting) are met for a status setting the monitor status is set to the corresponding status condition. If status conditions are met for more than one status condition setting the status of the monitor is set to the highest valued status condition. For example, if one condition selected as Error if and another condition selected as Warning if are both met, the status would be reported as an error, with **error** being the highest value, **warning** the next highest and **good** the lowest value. The status is displayed by color and a status icon in the SiteScope interface.

A change of status signals an event and acts as a trigger for alerts associated with the monitor or the group to which the monitor belongs. For example, if the selected Monitor detects that the system has become unavailable, the status change from good to error is used to trigger an alert on error.

A change of status may also effect the state of a dependency between monitors. For example, a monitor that detects a change that results in a error status may be a trigger to disable one or more other monitors that are dependent on the system.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the selected or use the following steps to change the monitor status thresholds for this monitor instance:

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting for this condition, click the **New Error If** button and repeat the steps above.

5 Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Mercury Business Availability Center Settings

You use the Mercury Business Availability Center Settings section to control what data a monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the options for **Logging to Mercury Business Availability Center** as described below.

Do not report to Mercury Business Availability Center

This option is used when you do not want the SiteScope monitor measurements for the subject monitor to be transferred to Mercury Business Availability Center.

Report everything (all monitors and all measurements)

This option sends all monitor data to Mercury Business Availability Center for each time that the monitor runs. This option enables the largest data transfer load.

Report monitor level data (no measurements)

This option sends only monitor category (error, warning, good), status string, and other basic data for each time that the monitor runs. No information on specific performance counters is included.

Report monitor level data and measurements with thresholds

This option sends monitor category (error, warning, good), status string, as well as performance counter data for any counters that have been set with thresholds (for example, Error If, Warning If, etc.). The data is sent for each time that the monitor is run.

Report status changes (no measurements)

This option sends only monitor category (error, warning, good), status string, and other basic data ONLY when the monitor reports a change in status. No information on specific performance counters is included. This option enables the smallest data transfer load.

Configuration Item Attachment Settings

Optionally, you can expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

3

Using Templates to Deploy Monitors

Speed and standardization are important to the efficient management of increasingly complex IT systems. The templates feature enables you to deploy standardized group and monitor configurations across multiple infrastructure elements with a minimal number of configuration steps.

This chapter describes:	On page:
About SiteScope Templates	44
Understanding Templates	45
Planning Templates	47
Creating Templates	48
Working with Template Variables	53
Counter Selection in Monitor Templates	60
Using Templates to Deploy SiteScope Monitoring	65
Exporting and Importing Templates	66

About SiteScope Templates

Many business system environments consist of a large number of similar or redundant elements. Standardization of hardware and software facilitates system management. Monitoring the availability of these systems generally requires duplicated sets of monitors including more than one type of monitor. For example, if there are 50 servers in the infrastructure, the same key system resources, such as CPU, disk space, and memory, can be monitored for each server even though the applications that are running on each server may be different. Templates help speed the deployment of monitors across the enterprise through standardization of group structures, monitor types and configuration settings.

You create templates within a template container in the monitor tree in Monitor Administration. These elements are then displayed in the monitor tree where you can access them for changes or deployment. See "Understanding Templates" for more information.

You use templates to deploy a standardized pattern of monitoring to multiple elements in your infrastructure. Effective development and use of templates requires some planning. See "Planning Templates" for more information.

You create a template by adding and configuring groups, monitors, alerts, and variables to the template using actions similar to adding these elements to the monitor tree. Creating and referencing variables is an action that is unique to templates. See "Creating Templates" for more information.

You use template variables to as substitution markers for configuration settings that you want to change dynamically or interactively each time you deploy the template. Template variables use a special syntax. See "Working with Template Variables" for more information.

Several SiteScope monitor types use a measurement counter browser feature to dynamically query applications and systems for the metrics that are available for monitoring. When you create one of these monitors manually, you use a multiple step procedure to view and select counters. An alternative method is used to select counters when deploying templates. See "Counter Selection in Monitor Templates" for more information.

After you create and configure templates, you deploy them by using the monitor tree, action menus. You deploy templates using actions similar to copying and pasting monitor groups and monitors in the SiteScope hierarchy. See "Using Templates to Deploy SiteScope Monitoring" for more information.

Understanding Templates

Templates are objects you use to reproduce groups, monitors, and alerts according to a predefined pattern and configuration. Templates include group, monitor, and alert template objects as placeholders representing the type and configuration of corresponding items that you want to deploy in your monitoring environment. You then can deploy all of the items defined in the template in a single operation by copying the template to a location in the SiteScope hierarchy. Templates also use template variables that you use to interactively modify certain monitor and group configuration settings when you deploy the template.

You can create as many templates as you need. Once you have created a template, you can use it to deploy monitors as often as needed.

If SiteScope monitoring has not yet been configured and you are not familiar working with SiteScope monitors and groups, it is recommended that you set up some sample groups, monitors, and alerts before you create templates. This will help familiarize you with the monitor configurations and the relationship between monitors, groups, and alerts.

Template Objects

Templates are created and stored in a template container in the monitor tree. The template variable definitions and SiteScope objects configurable using the template are displayed as objects within the template element. The following table describes the objects used in templates.

Icon	Object Type	Description
	Template Container	A container you use to store and manage one or more templates. Template containers allow you to group and organize multiple templates in ways that describe their purpose or classification. Template containers are added only to the enterprise node.
	Template	A group you use to replicate monitoring deployment to multiple locations in the infrastructure. An individual template is comprised of the variable definitions and SiteScope object configurations that can be applied to the monitor deployment. You can add a template only to a template container node within the monitor tree.
	Template Variable	A variable designator that is used to prompt for user input during template deployment. Template variables are user defined or may include a pre-defined system variable that provides access to the list of remote server connections known to SiteScope. Template variables are added as children of the template container within which they are referenced.
	Template Configuration Objects	One or more group, monitor, and alert objects within a template. The monitor organization objects in the template are organized in the structure and relationship in which they will be created when the template is deployed. The icons for template configuration objects are the same as used for the objects deployed in the monitor tree.

Each template object includes a right-click action menu that you use to add, edit, or delete objects from the template.

Monitor elements added to a template are monitor configuration templates and not active monitor instances running against any system in the infrastructure. Monitors are only created and activated based on these configurations when you deploy the template outside the template container.

Planning Templates

Template planning is important for effective SiteScope management. You should consider the group and monitor relationships and properties in the template structure and how it will fit into the overall monitoring environment. The following are things to consider as you plan templates:

- **Monitor types** - Decide which monitors types you want to replicate using templates. Select monitor types that you need to monitor multiple systems. For example, CPU, Disk, Memory and Service monitor types are commonly deployed for each server in the infrastructure. You can also include multiple instances of the Service Monitor type in a template to monitor different services or processes running on each server.
- **Variable properties** - Decide which monitor configuration properties will need to vary from one template deployment to another. For example, the target server address or resource to be monitored is a common variable property. You should also consider what naming conventions you want to use for groups and monitors. You use template variables to enter or select values for variable properties each time you deploy the template. Not all monitor configuration properties can be configured using variables. See "Working with Template Variables" for more information.
- **Common properties** - For configuration properties that should be the same from one template deployment to another, you need to decide what the values should be. For example, the **Frequency** setting is a required setting for each monitor type. The default setting is 10 minutes. Depending on what is to be monitored and the overall monitor load, you may want to change this value so that monitors created by using the template will run more often.

- **Group structure** - Decide the group structure you want to use to organize the monitors. The organization groups and monitors in the template should be compatible with your overall plan for organizing the monitoring in your environment. The group structure you use may impact reporting, alerting, and monitor administration.
- **Alerts** - Decide if you will deploy alerts as part of the template. Consider which alert types and actions you want to associate with the groups and monitors. Alerts deployed as part of a template have their **Alert Targets** property set to all sibling elements to the element to which the alert is attached. For example, a template alert added to a group element will alert on any monitor added to the same group element. If this does not fit your alerting plan, you will need to edit the alert configuration after deployment or add alerts manually.

Creating Templates

The steps for creating SiteScope templates are similar to the steps you use to create other objects in SiteScope. The following sections describe the steps you use to create the hierarchy of objects used for templates:

- "Creating Template Containers and Templates" on page 48
- "Configuring Templates" on page 50

Creating Template Containers and Templates

All templates for creating monitors, groups, and alerts are stored in a template container. Template containers can be added only to the enterprise node in the monitor tree.

You can create multiple templates under a single template container object. Before creating template variables and configuring monitors, groups, or alerts for the template, you must create a template object in the monitor tree to store the configurations and associated variables.

To create a template container:

1. Right-click the enterprise node in the tree. The action menu opens.
2. Select **New Template Container**. The New Template Container screen opens in the content area.
3. Enter a name for the template container in the **Name** box. Maximum length: 250 characters.
4. Optionally, if there are any categories defined in this enterprise, you can assign a category to the template container under the **Category Settings** section.

   For details on defining categories, see "Working with Categories" in *Working with Monitor Administration*.
5. Optionally, you can assign a description to the template container under the **Advanced Settings** section. The description is displayed in the Contents tab for the enterprise node.
6. Click **Add** to create the template container.

   After you create a template container object you use the following steps to add a template object to the container. The template is the object into which you will add or create monitor and group configuration objects.

To create a template object:

1. Right-click a template container. The template menu opens.
2. Select **New Template** from the menu. The New Template screen opens in the content area.
3. Enter a name for the template in the **Name** box.
4. Optionally, if there are any categories defined in this enterprise, you can assign a category to the template under the **Category Settings** section.

   For details on defining categories, see "Working with Categories" in *Working with Monitor Administration*.
5. Optionally, if there are any advanced settings defined in this enterprise, you can assign a description of the object to the template container under the **Advanced Settings** section. The description appears only when editing or viewing the object properties.

6 Click **OK** to create the template. The name you entered appears in the monitor tree as a child node to the templates container.

Configuring Templates

The two methods for adding configurations to the created template are:

- ➤ copy an existing group and monitor hierarchy from a SiteScope to the template and edit the elements for use as a template
- ➤ manually enter the configurations you want to include in the template

---

Tip: If the SiteScope imported into Monitor Administration includes standardized monitoring examples, it may be easiest to copy that pattern from the SiteScope and convert the configurations to a template.

Copying Existing Configurations to a Template

Once you have created a template container, template, and template variables, you can add monitoring objects you have already configured to be used by the template. Use the following steps to create template elements by copying objects from an existing SiteScope container.

To copy existing SiteScope elements to a template:

1 Expand the SiteScope node and group nodes as necessary to locate the configurations you want to copy for the template.

2 Right-click the selected group, monitor, or alert. The object's action menu opens.

3 Choose **Copy** from the menu.

4 Right-click the template or group within the template folder to which you want to add the copied configurations. The template action menu opens.

5 Choose **Paste**. The copied element is added to the template as a child of the selected element.

6 If you are using template variables in the new template, edit each copied object by right-clicking the object and choosing **Edit** to replace the

applicable configuration field's value with the appropriate variable syntax. For details, see "Referencing Template Variables".

Manually Creating Template Configurations

If there are no applicable SiteScope monitor elements in your enterprise or if you want to create new structures or settings, you can create templates manually. You do this by adding groups, monitors, or alerts directly to a template.

Note: The following procedure creates a group element containing one or more monitors and subgroups groups. You can create a template containing multiple monitors that are not contained within a group. Such a template can only be deployed to an existing SiteScope group container; not directly to the SiteScope node.

To create a group within a template:

1. Right-click the template to which you want to add the group. To add a subgroup to an existing group in the template, right-click the applicable group element. The Template action menu opens.
2. Select **New Group** from the menu. The Add Template Group screen opens.
3. Enter a name for this group in the **Name** box. You can use a template variable in the **Name** box, enabling you to specify a unique name for the group when you deploy the template. For details, see step "Referencing Template Variables" on page 58.
4. Enter optional group settings in the **Advanced Settings** section. For details on configuring group settings, "Adding Groups to a SiteScope" in *Managing SiteScope*.
5. Optionally, if there are any categories defined in this enterprise, you can assign a category to the template under the **Category Settings** section.

   For details on defining categories, see "Working with Categories" in *Working with Monitor Administration*.
6. Click **OK** to add the group to the template.

To add a monitor to a template:

1. Right-click the group within the template into which you want to add the monitor configuration. The template group menu opens.
2. Select **New Monitor** from the menu. The New Monitor screen opens.
3. Select the monitor type you want to configure for the template. The New Monitor screen for that monitor type opens.
4. If you are using template variables, enter the variable syntax for all fields whose values are replaced with a variable. For details, see "Referencing Template Variables" on page 58.
5. Enter the actual values for any fields which remain constant throughout the template deployment. For details on configuring SiteScope monitors, see "Working with SiteScope Monitors" in *Configuring SiteScope Monitors*.
6. Click **OK** to add the monitor configuration to the template group.
7. Repeat these steps to add additional monitors to the template group.

To add an alert to a template:

1. Right-click the template group to add a group level alert. Right-click a monitor template to add an alert for that monitor. The template object's menu opens.
2. Choose **New Alert**. The New Alert screen opens.
3. Select the alert type whose definition you want to add to the template. The New Alert screen for that alert opens.

Note: Monitor Administration currently supports the Database, Disable or Enable Monitors, E-mail, Log Event, Pager, Post, SMS, SNMP Trap, Script and Sound alert types.

---

4. If you are using template variables, enter the variable syntax for all fields whose values are replaced with a variable. For details, see "Referencing Template Variables" on page 58.

5 Enter the actual values for any fields that remain constant throughout the template deployment. For details on configuring SiteScope alerts, see "Introducing SiteScope Alerts" in *Configuring SiteScope Alerts*.

6 Click **OK** to add the alert configuration to the selected template object.

Working with Template Variables

While you can create templates without using template variables, the use of variables is central to the power and utility of templates. Working with SiteScope template variables requires some planning and familiarity with the configuration settings used in SiteScope monitors.

Template variables are substitution markers for monitor configuration settings. You create template variables to represent monitor configuration settings that you want to be able to modify whenever you deploy the template. You reference the variable in a property text field in one or more template monitors. Examples of common uses for template variables are: server or host addresses, disk drive designators, file paths, and monitor name descriptions.

There are two steps you use when working with template variables:

1 Create the template variable in the template. See "Creating Template Variables" for more information.

2 Reference the variable in one or more configuration objects in the template. See "Referencing Template Variables" for more information.

Each variable that is referenced in a monitor or group object in a template will prompt the display of a corresponding entry field when the template is deployed. The variable name is used as a label for the text entry field.

Some monitor configuration settings can not be set using template variables. With the exception of the remote server selection menu, configuration items that are normally selected using a selection drop-down can not be defined using template variables. Configuration items that are normally selected using a check box or radio selection can not be configured using template variables.

Template variables are always child elements of the template container in which they reside. Variables can be referenced and used to define configuration settings for group, monitor, or alert configuration templates within the template.

You should plan and create the template variables you will use before you add groups and monitors to a template. This way you can enter the references to the variables into the template monitors, groups, or alerts as you add them to the template. Deleting a template variable that has already been referenced in a template monitor configuration may require that the referencing monitor be deleted from the template in order to clear the broken reference.

Variable Syntax

There are two types of template variables in SiteScope:

- **user-defined variables**
- **system variables**

User-defined variables are used to enter text-based values during template deployment. System variables are a set of predefined variables you use to access the list of remote servers known to SiteScope and system time information. Each type of variable has specific syntax conventions which are described in the following sections.

Syntax for User-Defined Variables

User-defined template variables can be alphanumeric characters and may contain the underscore character. They may not contain whitespace, punctuation marks, or other non-alphanumeric characters, except the underscore character. You can create as many variables as you need.

Examples of valid template variable syntax are:

description_text

DiskDrive

TARGET_URL

matchExpression

You should choose variable names that describe the configuration parameter that is represented. The variable name will be used as a label for the variable entry field on the variable value entry screen when you deploy the template.

Syntax for System Variables

SiteScope recognizes several pre-defined template variables. These are values that are known by the system, including the list of servers for SiteScope, detected servers such as NetBIOS, as well as user-defined server connection profiles such as remote Unix. The syntax and description for the pre-defined system variables are:

Syntax for System Variables	Description
SERVER_LIST	Returns a list from which to select one of all the servers known by the platform. Use this to allow selection of remote servers for **Server** or **Host Name** properties only.
SERVER_NAME	This variable is derived from the SERVER_LIST variable. Returns the name of the current server with \\ (backslashes) before the name. Use when referencing the server in other fields.
SERVER_NAME_BARE	This variable is derived from the SERVER_LIST variable. Returns the name of the current server without \\ (backslashes) before the name. Use when referencing the server in a field requiring just the name of the server (for example when deploying CPU monitors or when referencing the name of the server in a description: "Disk space on server Mail."
DATE	Returns the system date on the server where SiteScope is running. Use to add the date that a monitor was created to a name or description.
TIME	Returns the system time on the server where SiteScope is running. Use to add the time that a monitor was created to a name or description. The value will be the time when the template is actually deployed.

Important: The SERVER_LIST variable is the only system variable that must be added explicitly to templates. The other system variables are derived or can be accessed directly by referencing them in the target monitor or group configuration template. See "Referencing Template Variables" for more information.

Creating Template Variables

Template variables can only be added to a template object. Use the following steps to create template variables in a template.

To create a template variable:

1. Right-click the template into which you want to add the variable. The template menu opens.
2. Choose **New Variable** from the menu. The New Template Variable screen opens.
3. Enter a variable name in the **Name** box. This name is used to identify the variable in the template on the monitor tree. This is also the name that must be used as the substitution variable in the variable syntax. For details, see "Working with Template Variables".

Note: The name of a variable cannot be edited once the variable has been added. To change a variable name, delete the variable and create a new one with the correct name.

---

4. Enter a text description in the **Description** box. This description is displayed along with an entry field when deploying the template.
5. Optionally, enter a default value in the **Default Value** box to be used for this variable substitution. If you do not enter a value in this field and the field requires a value, you will be prompted to enter a value when deploying the template.
6. Click **OK** to add the variable definition to the template.

Referencing Template Variables

After you have added template variables to a template, you must create references to them in a monitor or group configuration object. The syntax you use to reference a variable will depend on the type of variable.

You reference a user-defined variable using the following syntax in the object's configuration field:

%%variable_name%%

The reference is both case sensitive and syntax sensitive. The variable_name reference must match the template variable name and be surrounded by double % symbols.

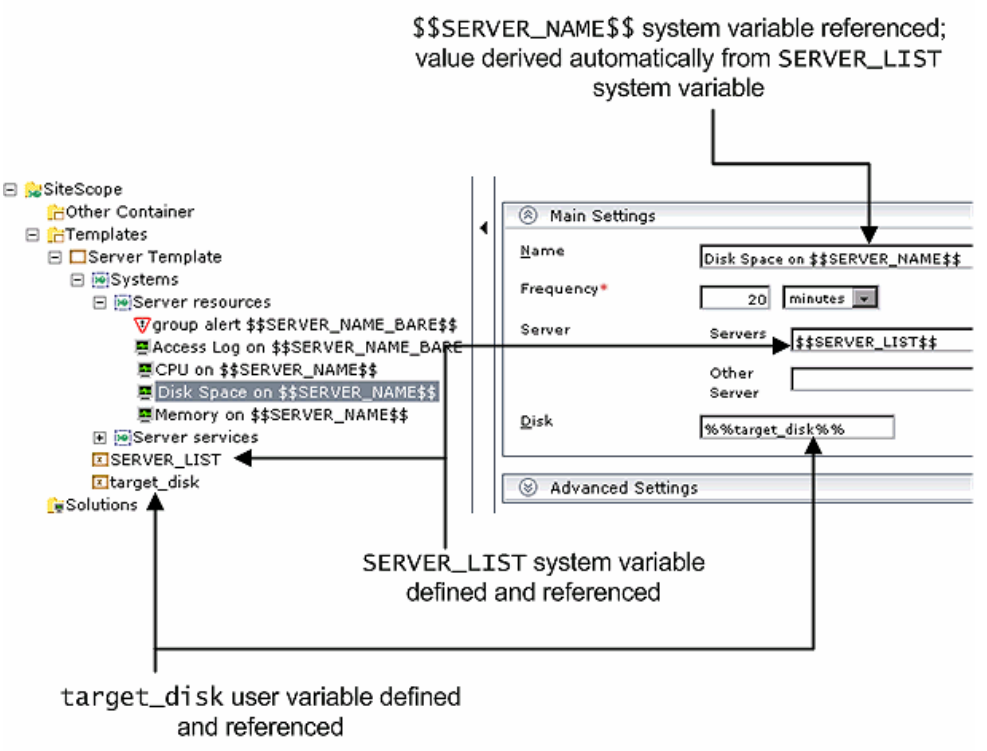
Note: User-defined template variables must be created before they can be referenced in monitor or group configuration templates. Using the %% symbols with a text string that has not already been added to the template as a template variable does not create a reference to a template variable even if a matching variable name is added later.

You reference a system variable using the following syntax in the object's configuration field:

$$VARIABLE_NAME$$

As with user-defined variables, the reference is both case sensitive and syntax sensitive. The SERVER_LIST variable must be defined explicitly as a variable in the template. As long as this variable is defined, the SERVER_NAME and SERVER_NAME_BARE variables may be used in configuration objects by referencing them using the $$VARIABLE_NAME$$ syntax directly in the monitor or group configuration object. The TIME and DATE variables can also be referenced directly.

The following diagram shows examples of how to reference user-defined variables and the SERVER_LIST and the derived system variables for a monitor template.



Counter Selection in Monitor Templates

SiteScope includes a number of application monitor types that are designed to monitor measurements specific to the target system. These monitor types use a **Get Counters** or **Get Measurements** browser feature in their properties panel. Configuring these monitor types manually requires several steps. After selecting the monitor type, you generally have to specify connection properties to the target system and then request SiteScope to retrieve the measurement counters from the remote system. The next step involves selecting the desired counters to be monitored and adding them to the configuration. After this, the monitor can be added to SiteScope.

Deploying monitors using templates does not accommodate a separate step for counter selection. Another mechanism is used to enable the selection of counters for these monitor types using templates. SiteScope uses text matching or regular expression matching to automate the counter selection step for template deployment. You do use a counter selection step when you create the template monitor.

The simplest method for counter selection in templates is to select the specific counters explicitly in the monitor template. This creates an explicit text match used to select the matching counter during deployment. You use the following steps to add a browsable counter monitor type with explicitly selected counters.

To add a monitor with browsable counters to a template:

1. Right-click the group within the template into which you want to add the monitor configuration. The template group menu opens.
2. Select **New Monitor** from the menu. The New Monitor screen opens.
3. Select the monitor type you want to configure for the template. The New Monitor screen for that monitor type opens.
4. If you are using template variables, enter the variable syntax for all fields whose values are to be replaced with a variable. This includes use of the SERVER_LIST system variable. For details, see “Referencing Template Variables” on page 58.

Note: You do not specify an actual server to connect to at this step of the procedure. You will need to enter valid server connection parameters in a following step.

---

5 Enter the actual values for any fields which remain constant throughout the template deployment. For details on configuring SiteScope monitors, see "Working with SiteScope Monitors" in *Configuring SiteScope Monitors*.

6 Depending on the monitor type, click the **Get Measurements** or **Get Counters** button in the lower portion of the Main Settings section of the Properties tab. The counter selection dialog box opens.

7 Depending on the monitor type, select a server or enter the connection information for a server that is running the service or application that you want to monitor. This may be a duplication of the information you entered for the monitor configuration.

8 When you have selected a valid server or entered the necessary connection information, click the **Get Measurements** or **Get Counters** button in the lower portion of the dialog box to retrieve the available counters. The counter selection dialog box is updated.

9 Select the measurements or counters that you want to monitor. These will be the counters configured for each instance of the monitor created when the template is deployed. Use the selection features as applicable to expand or browse the available counters and mark them for selection.

If the specific counters on the target system will vary from one deployment to another, you may be able to use a regular expression to match a pattern that represents the type or category of counter you want to monitor. See "Counter Selection Using Regular Expressions" on page 62 for more information.

10 Depending on the monitor type, click the **Add** button to add the selection to the selection list. Click the **OK** button to confirm the selection. The screen closes and the selected counters are displayed in the **Counters** section of the Main Settings panel.

11 Configure the other template monitor properties as applicable.

Note: Once you have selected counters for the template monitor, the counters become available as status threshold parameters in the Threshold Settings section.

---

12 Click **OK** to add the monitor configuration to the template group.

Counter Selection Using Regular Expressions

Many applications have a number of measurement counters that vary according to the system on which it is running, the configuration of system options, and the components installed. In this case, selecting explicit counters in a monitor template may not be useful across multiple instances of an application or system. Some systems have measurement counters that have a similar pattern but may vary by the name of a node or object context. You can use regular expressions in monitor templates to help automate the selection of multiple measurement counters.

Note: Use of this regular expression counter matching feature requires knowledge of the counters on the system to be monitored. You should manually set up a monitor of the type you want to add to the template and carefully review the counters available on the type of system you want to monitor. Creating a "greedy" regular expression that matches large numbers of counters on a remote system may adversely impact SiteScope performance.

The steps you use to create a template monitor to use regular expressions are very similar to the procedure described in the previous section. Instead of selecting all of the counters to be monitored explicitly, you select one or more counters that are representative of all the counters you want to select. The counter selections in monitor templates are stored as text strings. You edit these strings to create patterns that SiteScope will use to find matching counters that will be selected when the monitor is deployed.

Examples

➤ **Example 1.** The following is a simple example of how a regular expression can be used for counter selection for a SNMP by MIB Monitor type in a template:

You want to monitor the following three counters from several SNMP agents in your infrastructure:

```
iso/org/dod/internet/mgmt/mib-2/system/sysDescr
iso/org/dod/internet/mgmt/mib-2/system/sysUpTime
iso/org/dod/internet/mgmt/mib-2/system/sysName
```

You could select all three counters explicitly in the template monitor. Alternately, you could select one of these and then modify the counter string to be a regular expression such as the following:

```
/iso\/org\/dod\/internet\/mgmt\/mib-2\/system\/sys[DUN][a-zT]*/
```

In this example, the counter selection string has been edited to add a pair of / slashes before and after the string. This is necessary to indicate that the string is to be interpreted as a regular expression. Since the selection string included several / slash characters initially, each of these characters must be escaped by adding a \ backslash character immediately preceding it. The [DUN][a-zT]* string includes two character class declarations commonly used in regular expression syntax. See "Using Regular Expressions" in *Advanced Monitor Options* for more information on regular expression syntax.

➤ **Example 2.** The following is an example of how a regular expression can be used for counter selection for a Unix Resource Monitor type in a template:

You want to monitor daemon processes running on several Unix or Linux servers in your infrastructure. The list of processing running might include the following:

```
Process\-bash\NUMBER RUNNING
Process\../java/bin/java\NUMBER RUNNING
Process\./ns-admin\NUMBER RUNNING
Process\./ns-proxy\NUMBER RUNNING
Process\./ns-sockd\NUMBER RUNNING
Process\/bin/sh\NUMBER RUNNING
Process\/etc/init\NUMBER RUNNING
```

```
Process\/usr/apache/bin/httpd\NUMBER RUNNING
Process\/usr/lib/nfs/statd\NUMBER RUNNING
Process\/usr/lib/saf/sac\NUMBER RUNNING
Process\/usr/lib/saf/ttymon\NUMBER RUNNING
Process\/usr/lib/snmp/snmpdx\NUMBERRUNNING
Process\/usr/lib/ssh/sshd\NUMBER RUNNING
...
```

You can create a regular expression counter selection string to match only those processes that end with the letter "d". The following is an example regular expression to match this pattern:

```
/Process[\W\w]{5,18}d[\W]{1,2}NUMBER RUNNING/
```

As with Example 1, the counter selection string includes / slashes before and after the string to indicate that the string is a regular expression. The example process strings on the Unix server include combinations of \ back slash and / forward slash characters. Since these characters have special meaning in regular expressions, they would have to be escaped. This can be complicated since the process strings have many variations and combinations of these and other symbols. The example regular expression used here simplifies the expression by using character class declarations. The [\W] class is used to match punctuation marks. This will match on the \, -, :, and / characters that appear in some of the process strings without the need to escape the characters individually. See "Using Regular Expressions" in *Advanced Monitor Options* for more information on regular expression syntax.

Modifying Counter Selection Strings to Use Regular Expressions

You can modify counter selection strings for template monitors to use regular expressions when you create the monitor or you can edit the monitor later. You use the following steps to modify a template monitor to use a regular expression for measurement counter selection.

To modify a template monitor for regular expression counter matching:

1. If necessary, right-click the monitor template you want modify. The template monitor menu opens. Click **Edit** to open the template monitor properties view.

2 In the Main Settings panel, select a counter selection string that is representative of the pattern of counters you want to configure for the monitor. In the **Selected Measurements** or **Counter Name** section (depending on the monitor type), click the  button to the right of the counter string you want to edit. A string edit dialog opens.

3 Modify the counter selection string to be a regular expression by adding a slash (/)character to the beginning and end of the string. Modify the string to use other pattern matching syntax as appropriate. See "Using Regular Expressions" in *Advanced Monitor Options* for more information on regular expression syntax.

4 Click the **OK** button at the bottom of the edit dialog screen. The dialog box closes and the counter selection string is updated in the Main Settings panel.

If the template monitor was configured with explicit counter selections that can be matched using the regular expression that was entered, you can delete the extra counter strings by clicking the  button to the right of the counter string.

5 Click the **OK** button at the bottom of the monitor Properties tab to update the template monitor configuration.

Using Templates to Deploy SiteScope Monitoring

You deploy SiteScope monitoring using templates by a copy and paste operation within the monitor tree. The paste operation opens a template value dialog where you specify values for any template variables used in your template objects. You use the following steps to deploy templates.

To deploy a SiteScope monitor configuration template:

1 Expand the applicable template container in the monitor tree and select the template folder you want to deploy. Right-click the template. The template menu opens.

2 Choose **Copy**.

3 In the monitor tree, right-click the SiteScope node or SiteScope group container where you want to deploy the template. The container's menu opens.

4 Choose **Paste**. The Variable Values input screen opens in the content area. The entry fields displayed correspond to the template variables used in the template objects. For example, if there is a template variable named server_id which is used in a Disk Space and a Memory monitor defined in the template, an entry field labeled **server_id** will be displayed in the Variable Values input screen. The value you select or enter will be used for each monitor that references the server_id variable.

5 Enter the required variable values in the entry fields displayed.

If you used the SERVER_LIST pre-defined variable definition, the entry field is a list of available remote server values detected by the system. The system variables SERVER_NAME and SERVER_NAME_BARE return values based on the server selected in the **SERVER_LIST** item.

6 Click **OK** to finish the deployment.

Monitor AdministrationSiteScope makes the variable value substitutions, sends the configuration settings to the remote SiteScope, and adds the applicable elements to the monitor tree.

Exporting and Importing Templates

Templates can be exported for use on other SiteScope installations. This allows you to efficiently replicate standardized monitor configurations across the enterprise.

Note: SiteScope templates are stored as binary data. This is different than the text based monitor sets used in earlier versions of SiteScope. Any changes to templates must be performed using the SiteScope interface

---

You export and import templates by using a template container's action menu. One or more templates can be exported to a single file. You use the following steps to export templates from SiteScope.

To export templates from SiteScope:

1. Click the template container object in the left menu that contains the template or templates you want to export. The Export Template screen opens.
2. Enter a valid file name in the **Export File Name** field. Use a name that is descriptive of the template or templates to be exported.
3. The default location for exported templates is the <SiteScope_install_path>\SiteScope\export. To have the file saved to a different location, enter the location in the **File Path** field.
4. Use the Templates to Export menu tree to select the templates you want to export. By default, all templates within the template container will be exported. Use the check boxes to the left of the template names to select or deselect templates.
5. Click the **OK** button to export the templates. SiteScope creates an export file using the information you entered.

   Once you have exported templates, you can copy the export file to another SiteScope server and import the template configuration. Make a note of the exact filename and location where you copy the file. You use the following steps to import a template.

To import templates into SiteScope:

1. Click the template container object in the left menu into which you want to import the template or templates. The Import Template screen opens.
2. Enter the name of the file you want to import in the **Import File Name** field.
3. Enter the path to file to be imported in the **File Path** field. The default location for importing templates is <SiteScope_install_path>\SiteScope\export.
4. Click the **OK** button to export the templates. Templates contained in the file are added to the template container. The imported templates can be used directly or modified as needed.

4

Monitor Deployment Wizard

The Monitor Deployment wizard enables you to deploy SiteScope monitors onto configuration items in the CMDB using pre-defined templates.

This chapter describes:	On page:
Monitoring Configuration Items with the Monitor Deployment Wizard	69
Using the Monitor Deployment Wizard	71
Configuring Settings for the Wizard	75
Template Reference and Monitor Tree Objects	75

Monitoring Configuration Items with the Monitor Deployment Wizard

When working with configuration items, you may want to deploy SiteScope monitors onto those configuration items that can be monitored. For details on understanding configuration items, see "Introduction to CMDB Administration" in *Working with the CMDB*.

The CMDB may already include CI data that can be used for monitor deployment. These properties may have been entered while adding the configuration item to the IT Universe model or may have been discovered by the Discovery Manager. For details, see "Populating the IT Universe Model" in *IT Universe Administration*.

Mercury Business Availability Center enables you to use that data to configure SiteScope monitors for existing CIs in the CMDB using the Monitor Deployment wizard.

The Monitor Deployment wizard:

- recognizes onto which configuration items a SiteScope monitor can be deployed
- recognizes which monitors to deploy onto which configuration items
- enables you to select available monitor templates to deploy onto selected CIs
- deploys monitors using templates
- imports the configuration item's properties that have been defined in CMDB Administration into the monitor's properties
- uses template variables to enable you to enter data for monitor properties that are not imported from the configuration item's definition
- creates in the CMDB a **monitored by** relationship between the monitored CI and the created monitor

Example of Monitor Deployment

For example, an Oracle database has been added as a CI to the IT Universe model in CMDB Administration. In Monitor Administration, you can use the Monitor Deployment wizard to deploy the Oracle Database monitor onto the CI. The wizard imports the following properties that are defined for the server in the CMDB:

- database server IP address or server name

The wizard prompts you to enter values for the following variables that are necessary for the deployment of the monitors:

- database user name
- database password
- database port
- database SID
- database driver

Using the Monitor Deployment Wizard

You access the Monitor Deployment wizard in Monitor Administration. The wizard is accessible only if you have a running SiteScope attached to Monitor Administration.

You deploy monitors using the Monitor Deployment wizard only onto those configuration items that are not yet attached to a monitor CI. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

To use the Monitor Deployment wizard:

1. Access Monitor Administration by selecting **Admin** > **Monitors**.
2. Select from the following options in the monitor tree:
   - ➤ Right-click the SiteScope server or group that will run the Monitor Deployment monitors. The SiteScope menu opens. Select **Monitor Deployment Wizard**.
   - ➤ Highlight the SiteScope server or group that will run the Monitor Deployment monitors and click the **Monitor Deployment Wizard** button at the top of the Contents page.

   The Monitor Deployment wizard opens to the Welcome page.
3. Click **Next** to begin the wizard.

   When you click Next to begin the wizard, the Source Manager synchronizes the SiteScope adapter to update all monitor data. This may take a few minutes depending on how many SiteScope monitors are deployed in your environment and when the last synchronization took place.

   Once synchronization is completed, the Select Configuration Items to Monitor page opens.
4. In the left pane of the Select Configuration Items to Monitor page, select a view in the View Explorer.

   For details on working in the View Explorer, see "Using View Explorer" in *Working with the CMDB*.
5. Within the selected view, highlight one or more CIs onto which to deploy the SiteScope monitors. You can also select the entire view.

6. Click the right arrow to move the selected CIs to the right pane.

   The table in the right pane lists in a tree hierarchy all the CIs that are in your selection, including both those CIs for which Monitor Deployment creates monitors and those for which the wizard does not create monitors.

   The wizard cannot create monitors for the following CIs:

   - CIs that already have attached monitors
   - CIs that do not have a matching template for deploying a monitor type
   - CIs that are monitor CIs, generally those appearing in the monitor view

   If any CIs in the right pane fall into any of these categories, the CI appears in the right pane with a tooltip indicating why monitors are not created for the CI in the wizard.

7. Optionally, view all the CIs in the selected CI tree by clicking the plus sign to the right of the CI to expand each CI level.

8. Optionally, modify your selection of CIs by removing CIs from the selected CI table in the right pane. Select the CI and click the left arrow button.

9. When the selected CI list in the right pane reflects the CIs for which you want to deploy monitors, click **Next**. The Select Templates to Apply page opens.

   The left pane lists all the available templates in the wizard. The child objects are the monitors that are deployed by the template. The right pane lists the CI Types of all the CIs selected in the previous page.

   If the wizard was able to match templates to the selected CI Types, the CI Type is listed with the applicable template as a child object.

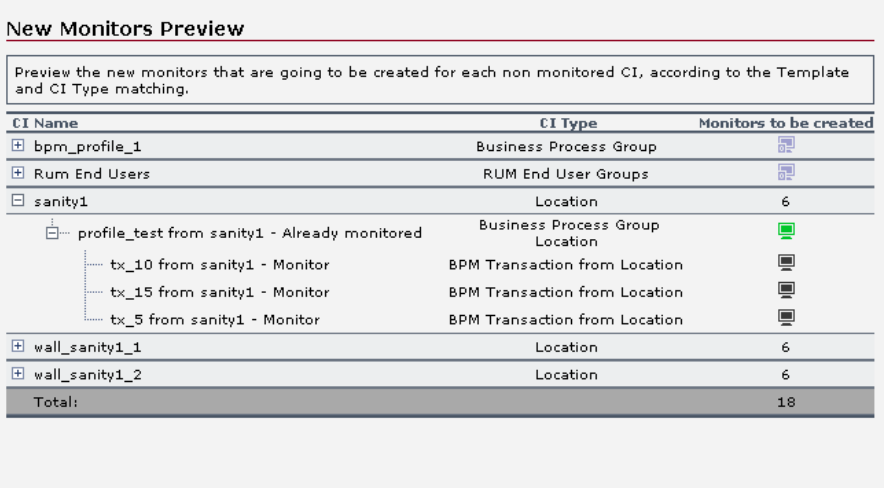
10. Optionally, to apply further templates to CI Types not automatically matched by the wizard:

    a. In the left pane, select the templates that you want to apply to the selected CI Types. You can select multiple templates by pressing CTRL.

    b. Once all the required templates are highlighted, click the right arrow to apply the templates to the CI Types. The templates appear as child objects of the CI Type.

    To reset the list and remove all the templates from the CI Types, click **Reset**.

11 Click **Next**. The New Monitors Preview page opens.



New Monitors Preview

Preview the new monitors that are going to be created for each non monitored CI, according to the Template and CI Type matching.

CI Name	CI Type	Monitors to be created
⊞ bpm_profile_1	Business Process Group	
⊞ Rum End Users	RUM End User Groups	
⊟ sanity1	Location	6
⊟ profile_test from sanity1 - Already monitored	Business Process Group Location	
tx_10 from sanity1 - Monitor	BPM Transaction from Location	
tx_15 from sanity1 - Monitor	BPM Transaction from Location	
tx_5 from sanity1 - Monitor	BPM Transaction from Location	
⊞ wall_sanity1_1	Location	6
⊞ wall_sanity1_2	Location	6
Total:		18

The table lists each selected CI with its CI Type. The Monitors to be created column indicates with an icon whether a monitor is being created for the CI as follows:



➤ black monitor icon indicates a monitor to be created



➤ green monitor icon indicates that a monitor is already attached to this CI and, therefore, no monitor is created



➤ blue monitor icon indicates that the CI Type has no matching template for monitor deployment

For parent objects, a value representing the sum of monitors to be created for all its child objects is displayed.

If no monitor is created, a tooltip over the monitor icon explains why.

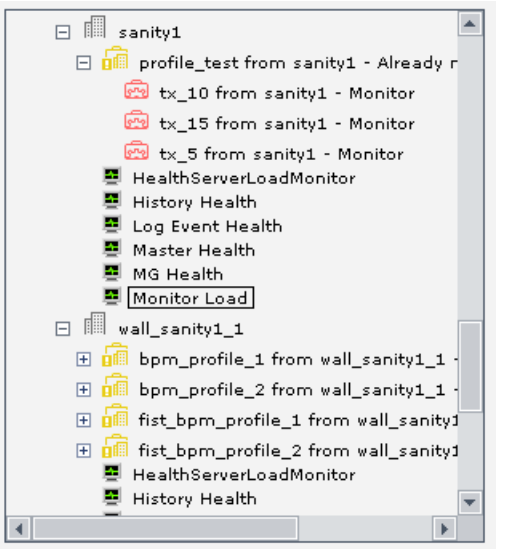
12 In the table, review the list of CIs and monitors to be created. If the list reflects an accurate monitor deployment, click **Next**.

In some cases, the wizard is able to import all the data required for deploying the monitor. In this case, the Review Configuration Summary page opens automatically and you can continue from step 15.

If any monitors require values for the template variable, an Enter Required Data for CI page opens for each selected CI that requires data.

13 For each selected CI for which monitors are created with missing data, enter the required data for the template variable to create the applicable monitors.

14 Click **Next** for each CI page. When all required data is entered, the Review Configuration Summary page opens.



15 To view the CIs and their respective monitors, expand the parent objects in the table listing all the CIs.

16 Click **Finish** to deploy the monitors.

Configuring Settings for the Wizard

The Monitor Deployment wizard includes several settings that can be modified to change the default limitations of the wizard. You modify these settings in the Infrastructure Settings page. To access the Infrastructure Settings page select **Admin** > **Platform** > **Infrastructure Settings** > **Foundation** > **Monitor Administration**. For details on the Infrastructure Settings page, see "Infrastructure Settings" in *Platform Administration*.

These settings include:

- maximum number of CIs to select in the wizard. The default is 5,000 CIs.

  If the maximum is exceeded, the monitors cannot be deployed and a corresponding message opens.

- maximum number of monitors to deploy in the wizard. The default is 100 monitors.

  If the maximum is exceeded, the monitors cannot be deployed and a corresponding message opens.

- maximum number of CIs to view in the Review Configuration Summary page. The default is 1,000 CIs.

  If the maximum is exceeded, the Review Configuration Summary page lists the CIs in a flat list and not in a tree hierarchy.

Template Reference and Monitor Tree Objects

The Monitor Deployment wizard is enabled by a series of templates pre-configured in your monitor tree in Monitor Administration.

Monitor Tree Objects

The Monitor Deployment templates appear by default in the monitor tree in a container called **Monitor Deployment**. This container and the templates and variables within it should not be edited or deleted. For details on the monitor tree and monitor tree objects, see "Using Monitor Administration" in *Working with Monitor Administration*.

Only advanced users with a thorough knowledge of working with templates should attempt to edit any of the variables or to add variables to the templates. For details, see "Using Templates to Deploy Monitors" on page 43.

The monitor tree also includes a category called **Monitor Deployment** that appears in the Category Settings area for every object in the monitor tree. Within this category are the category values that the wizard uses to deploy the monitors. These categories should not be edited or deleted. (For general information on monitor tree categories, see "Working with Categories" in *Working with Monitor Administration*.)

Template Reference

Following is a table listing all the configuration items onto which the Monitor Deployment wizard can deploy monitors. The table includes information regarding onto which CIs you can deploy monitors, which monitors are deployed, the monitor properties imported from the CMDB, and the variable definitions that are either imported from the CMDB or defined during the wizard.

Configuration Item Template	CI Type	Applicable Monitor	Discovered Properties	Variables
Apache server	Apache	Apache Server monitor	server name or IP address	application_IP
			application port (default value is 8080)	application_port
IIS server	IIS	IIS Server monitor	server name or IP address	application_IP

Configuration Item Template	CI Type	Applicable Monitor	Discovered Properties	Variables
Host	Host	Ping monitor	dns name	host_dnsname
	NT			
	Unix			
	Network			
	Switch			
	Router			
	switch-router			
NT server	NT	Windows Resources monitor	dns name	host_dnsname
Unix	Unix	CPU monitor	dns name	host_dnsname
		Memory monitor	dns name	host_dnsname
SQL server	sqlserver	SQL Server monitor	server name or IP address	application_IP
		Service monitor	server name or IP address	application_IP

Configuration Item Template	CI Type	Applicable Monitor	Discovered Properties	Variables
Oracle database	oracle	Oracle Database monitor	server name or IP address	application_IP
			database password (default value is manager)	database_dbpassword
			database port (default value is 1521)	database_dbport
			database SID	database_dbsid
			database user name (default value is system)	database_dbusername
			driver (default value is oracle.jdbc.driver.Oracle.Driver)	driver

Part II

Solution Templates

5

Introducing SiteScope Solution Templates

The range of monitor types available with SiteScope gives you flexibility in monitoring a variety of systems and services. With the increasing complexity of current network applications, it is difficult to know the most effective way to monitor key systems and services. SiteScope solution templates are designed to provide rapid deployment of performance and availability monitoring optimized for specific applications and services.

This chapter describes:	On page:
About Solution Templates	81
Working with Solution Templates	82

About Solution Templates

Solution templates are special monitor set templates designed to monitor popular enterprise applications and network systems. You use solution templates to deploy a combination of standard SiteScope monitor types and solution-specific monitors with settings that are optimized for monitoring the availability, performance, and health of the target application or system. For example, the solutions for Microsoft Exchange monitoring include performance counter, event log, and Exchange application specific monitor types.

The following table lists solution templates available for SiteScope. The following sections contain more information about each solution and the solution specific monitor types.

Solution Name	Description
Active Directory Solution Template	Monitors the performance and efficiency of Microsoft domain controllers.
Exchange Solution Templates	Includes individual solution options for monitoring application health, message flow, and usage statistics for Exchange Server 5.5, Exchange Server 2000, or Exchange Server 2003.
Oracle Solution Template	Monitors performance, availability, and usage statistics for Oracle 8i, 9i and 10g databases.
SAP Solution Templates	Monitors performance, availability, and usage statistics for SAP system components.
Siebel Solution Templates	Monitors performance, availability, and usage statistics for Siebel Application Server installed on Microsoft Windows operating systems.
WebLogic Solution Template	Monitors performance, availability, and usage statistics for BEA WebLogic Server 6.x, 7.x and 8.x application servers.
WebSphere Solution Template	Monitors performance, availability, and usage statistics for IBM WebSphere Server 5.x application servers.

Working with Solution Templates

The following is an overview of the steps for deploying solution templates:

1. Request the applicable Solution license from Mercury Customer Support.
2. Enter the license into the SiteScope product using the General Preferences page.
3. Open or create a monitor group into which you want to deploy the solution monitors.

4. Select the applicable solution template.
5. Copy and paste the solution template to the target monitor group container.
6. Complete the Solution Template Variable Values page as indicated.
7. Configure alerts and reports for newly created solution monitors.

6

Active Directory Solution Template

To address the needs of Active Directory performance monitoring, Mercury offers the Active Directory Solution. The SiteScope Active Directory Solution provides monitoring of domain controller performance, services on which Active Directory depends, and distributed Active Directory performance.

This chapter describes:	On page:
Understanding the Active Directory Solution	85
Deploying the Active Directory Solution Template	87

Understanding the Active Directory Solution

The Active Directory Solution Template deploys a set of monitors against a particular Domain Controller. These monitors encompass best practices monitoring for Active Directory. This template includes NT Event Log, Service, LDAP, performance counter and Active Directory Replication monitors.

Note: You must have the applicable SiteScope option license to use the Active Directory solution templates. Contact your Mercury sales representative for more information about Solution licensing.

The purpose of a solution template is to provide comprehensive monitoring without requiring the SiteScope user or the IT organization to be experts on the application.

Benefits of the Active Directory Solution Template include:

- Reduces the need for Active Directory performance domain expertise
- Reduces the time to configure and deploy Active Directory monitors
- Helps identify both real-time performance bottlenecks and longer term trends
- Adds no overhead to production systems

The Active Directory Solution Template deploys monitors that target the following aspects of Active Directory performance:

- **Domain controller performance**
  This category refers to the low level health of each domain controller in the environment. The Active Directory Solution Template automatically configures monitors for domain controller health.
- **Dependent services**
  Active Directory depends on several key services. Without these services, Active Directory can become unresponsive or fail altogether. The Active Directory Solution Template automatically configures monitors for a list of important services upon which Active Directory performance is dependent.
- **Distributed Active Directory performance**
  Perhaps the most important aspect and key indicator of Active Directory performance is how fast Active Directory is replicating changes out to all domain controllers. The Active Directory Solution Template automatically configures monitors for monitoring and testing replication of changes and updates.

An in-depth description of the Active Directory Solutions is available as a separate document as part of the SiteScope installation. This document can be found at **<SiteScope root directory>\sisdocs\pdfs\SiteScope_Active_Directory_Best_Practices.pdf**.

Note: This is a password protected document. The password is provided along with the Active Directory Solution license key from Mercury.

After the solution template is deployed the monitors created will behave the same as other monitors in SiteScope. This means that they can be viewed, edited, and deleted like other monitors.

Note: Some of the monitor types deployed by the solution templates can only be added to SiteScope by using the Active Directory Solution sets. See the section for the particular monitor types for more information.

Deploying the Active Directory Solution Template

Deploy one Active Directory Solution Template for each domain server in your environment. Use the following steps to deploy an Active Directory Solution Template.

To deploy an Active Directory Solution Template:

1. Click on the SiteScope container into which you want to add the Active Directory Solution and expand the container to display the group containers.
2. Right-click the Active Directory Solution template icon to display the action menu and select **Copy**.
3. Select the SiteScope container or the monitor group container into which you want to deploy the Active Directory Solution.
4. Right-click on the container to display the action menu and select **Paste**. The Variable Values form opens in the contents panel.
5. Complete the items on the Active Directory Solution Variable Values form as described in the section Active Directory Solution Template Settings below. When the required items are completed, click the **OK** button.
6. As SiteScope creates the monitors, a paste results message is shown listing the names of the monitors created along with messages indicating success or error. After the monitors have been created, select **Close**.

   Deploying the Active Directory Solution creates a new monitor group container in which the individual solution monitors are added.

Note: Errors detected during the creation of monitors using a solution template are independent of the status returned when the individual monitors are run. This means that the monitors may be created successfully but that the configuration settings may be incorrect or that the system being monitored is unavailable.

Note: Solution templates do not configure any automated alerts for the monitors created. You must create and associate one or more alert definitions to the monitors or monitor groups created by solution templates.

Active Directory Solution Template Settings

Server_List

Choose the Domain Controller that you want to monitor. Click the **choose server** link to monitor services or processes on another server (may require that you define connections to other servers).

Host_Name

Type in the host part of the domain controller's hostname (do not include the fully qualified domain name).

Replicating_Domain_Controllers

Type in a comma separated list of domain controllers that replicate data from the domain controller selected above.

LDAP_Security_Principal

Enter in LDAP Security Principal of a Domain Admin account. For Active Directory this is in the format of cn=Domain Admin User,cn=users,dc=yoursite,dc=com.

Password

Enter in the password for the user selected above.

Logical_Drive

Enter in the logical drive that this Domain Controller is using for its database and log files.

Global Catalog (AD with Global Catalog ONLY)

If the Domain Controller is a Global Catalog server then check this box.

7

Exchange Solution Templates

To address the needs of Microsoft Exchange performance monitoring, Mercury Interactive offers Exchange solutions. The SiteScope Exchange Solution Templates provide monitoring of performance, availability, and usage statistics for Microsoft Exchange 5.5, 2000, and 2003 servers.

This chapter describes:	On page:
Understanding the SiteScope Exchange Solution	91
Deploying Exchange Solution Templates	94

Understanding the SiteScope Exchange Solution

The SiteScope Exchange Solution includes three solution templates that implement best practice monitoring for Microsoft Exchange messaging services. This includes solution templates for the following:

- Exchange 5.5
- Exchange 2000
- Exchange 2003

You use these solution templates to deploy a set of monitors that test the health, availability, and performance of an Exchange server. Depending on the set chosen, this set includes monitors checking NT Event log entries, MAPI operations, system performance counters, and message system usage statistics.

Note: You must have the applicable SiteScope option license to use the Exchange Solution templates. Contact your Mercury sales representative for more information about Solution licensing.

The Exchange Solution templates provide comprehensive Exchange system monitoring without requiring the SiteScope user or the IT organization to be experts on the application.

Benefits of the Exchange Solution templates include:

- Reduces the need for Exchange performance domain expertise
- Reduces the time to configure and deploy Exchange monitors
- Helps identify both real-time performance bottlenecks and longer term trends
- Adds no overhead to production systems

The Exchange solution templates deploy monitors that target the following aspects of Exchange performance and health:

- **Basic server/OS performance**
  This category refers to the system-level health of a server. The Exchange Solution Template automatically configures monitors for server health.
- **Application performance**
  Application performance is a measure of how well specific Exchange components are functioning. The Exchange Solution Template automatically configures monitors for a list of important Exchange application components.
- **Mail protocol response time**
  Perhaps the most important aspect and key indicator of Exchange performance is mail protocol response time. While Exchange can utilize many protocols, the MAPI protocol is commonly used in Microsoft networks.

➤ **Usage statistics**
The last category related to Exchange performance is usage. While usage in and of itself is not necessarily a key indicator of performance, changes in usage can affect overall Exchange performance. In addition, Exchange usage statistics help IT organizations spot trends and plan for the future. The Exchange Solution Template automatically configures monitors for a list of important Exchange usage parameters.

An in-depth description of the Exchange Solutions is available as a separate document as part of the SiteScope installation. This document can be found at **<SiteScope root directory>\sisdocs\pdfs\SiteScope_Exchange_Best_Practices.pdf**.

Note: This is a password protected document. The password is provided along with the Exchange Solution license key from Mercury.

After the solution template is deployed the monitors that are created will behave the same as other monitors in SiteScope. This means that they can be viewed, edited, and deleted like other monitors.

Note: Some of the monitor types deployed by the solution templates can only be added to SiteScope by using the Exchange Solution templates. See the section for the particular monitor types for more information.

System Requirements

The Exchange Solution license must be applied to the SiteScope server onto which you want to deploy the Exchange Solution. See the section on SiteScope General Preferences for details on how to enter license information.

Important: Each of the Exchange solutions make use of the SiteScope MAPI Monitor. Successful deployment of this monitor type requires specific setup configuration relating to the mailbox owners and the SiteScope service. See the "System Requirements" for the MAPI Monitor for the steps you need to perform before deploying an Exchange Solution Template.

Deploying Exchange Solution Templates

Deploy one Exchange Solution Template for each Exchange server in your environment. Use the following steps to deploy an Exchange Solution Template.

To deploy an Exchange Solution Template:

1. Click on the SiteScope container into which you want to add the Exchange Solution and expand the container to display the group containers.
2. Select the Exchange Solution template that matches the version of Microsoft Exchange that you want to monitor.
3. Right-click the solution template icon to display the action menu and select **Copy**.
4. Select the SiteScope container or the monitor group container into which you want to deploy the Exchange Solution.
5. Right-click on the container to display the action menu and select **Paste**. The Variable Values form opens in the contents panel.
6. Complete the items on the Exchange Solution Variable Values form as described in the section "Exchange Solution Template Settings" below. When the required items are completed, click the **OK** button.
7. As SiteScope creates the monitors, a paste results message is shown listing the names of the monitors created along with messages indicating success or error. After the monitors have been created, select **Close**.

Deploying the Exchange Solution creates a new monitor group container in which the individual solution monitors are added. The monitor group container is assigned a name of the format Exchange *version_number* on *server_name* where *server_name* is the server selected from the **Server_List** field.

Note: Errors detected during the creation of monitors using a solution template are independent of the status returned when the individual monitors are run. This means that the monitors may be created successfully but that the configuration settings may be incorrect or that the system being monitored is unavailable.

Note: Solution Templates do not configure any automated alerts for the monitors created. You must create and associate one or more alert definitions to the monitors or monitor groups created by solution templates.

Exchange Solution Template Settings

Server_List

Choose the server on which the Exchange server that you want to monitor is running from the selection list. If the server you want to monitor is not in the list you will need to define a connection profile to the server. See the section on Monitoring Remote Windows Servers for the steps you use to create a Windows connection profile.

Mail_User

Enter the Windows account login name for the user for which e-mail round trip times will be tested using MAPI.

Mail_Password

Enter the Windows account login password for the user name entered above.

Mailbox

Enter the name (alias) of the mailbox to be used for testing e-mail round trip times using MAPI. This is often the e-mail account name but it may be a different name. It is recommended that you copy the mailbox name as it appears in the E-Mail Account properties for the e-mail account you will be using for this solution.

Mail_Domain

Enter the domain to which both the owner of the mailbox being used and the Microsoft Exchange server belong.

Note: The owner of the mailbox to be used by this solution must also have administrative account privileges on the machine where SiteScope is running. SiteScope also needs user account access to the domain where the Microsoft Exchange server is running.

WMI_User (Exchange 2003 ONLY)

Enter the username to use when querying the server for mailbox and public folder statistics. The statistics are gathered via WMI (Windows Management Instrumentation), so the username entered here must have permissions to read WMI statistics on the server from WMI namespace root\MicrosoftExchangeV2. If this field is left blank, the user that SiteScope is running as will be used.

WMI_Password (Exchange 2003 ONLY)

Enter the password for the user entered above for gathering WMI statistics, or leave this blank if user field is left blank.

8

Oracle Solution Template

To address the needs of Oracle database performance monitoring, Mercury offers the Oracle Database Solution. The SiteScope Oracle Database Solution provides efficient and thorough monitoring of performance, availability, and usage statistics for Oracle 8i, 9i and 10g databases.

This chapter describes:	On page:
About the Oracle Database Solution	97
Deploying Oracle Database Solution Templates	99
Oracle Database Solution Tools	103
Understanding Oracle Database Solution Tools	103

About the Oracle Database Solution

This solution uses a new monitor type called the Database Counter Monitor. This monitor collects performance metrics from JDBC-accessible databases. In addition to the new monitor type, you can use the Oracle Database Solution Template to deploy a collection of monitors configured with default metrics. These built-in default monitors and metrics use monitoring configurations have been researched from best practice data and expertise from Mercury's professional services organization, customers and industry experts.

Note: You must have the applicable SiteScope option license to use the Oracle Database Solution Template. Contact your Mercury sales representative for more information about Solution licensing.

The purpose of a solution template is to provide comprehensive Oracle database monitoring without requiring the SiteScope user or the IT organization to be an expert on the application. An in-depth description of the Oracle Database Solutions is available as a separate document as part of the SiteScope installation. This document can be found at **<SiteScope root directory>\sisdocs\pdfs\Sitescope_Oracle_Database_Best_Practices.pdf**.

Note: This is a password protected document. The password is provided along with the Oracle Database Solution license key from Mercury.

Benefits of the Oracle Database Solution Template include:

- Reduces the need for Oracle performance domain expertise
- Reduces the time to configure and deploy Database Counter Monitors against Oracle databases
- Helps identify both real-time performance bottlenecks and longer term trends
- Ensures that SiteScope monitoring license points are not wasted on lower priority monitors and metrics

The Oracle Database Solution Template deploys monitors that target the following aspects of Oracle performance and health:

General System Statistics

The most important V$SYSSTAT statistics are monitored by default in the monitors deployed by the Oracle Database Solution. Where applicable, these metrics are combined to calculate deltas and rates on a per-second or per-transaction basis. When monitoring the important metrics from the V$ tables in the database, the Oracle Database Solution is a replacement for manually generated SQL scripts.

Oracle Logs

Important Oracle log files are monitored for "ORA-" errors. Users may customize the these monitors to look for specific text in a log file, depending on their database configuration.

Diagnosing Database Problems

In addition to the deployed monitors, the Oracle Solution offers several tools which can be used to gain diagnostic information about a database. Resource-intensive SQL statements, shared server process contention, and the number of sessions waiting for specific events are all examples of the diagnostic data that these tools can provide. Since the tools are made available in the form of disabled monitors, this important information is literally just a click away.

Deploying Oracle Database Solution Templates

The SiteScope Oracle Database Solution Template facilitates the implementation of best-practice monitoring of Oracle Databases with a minimum of configuration. This solution can be used with Oracle 8i, 9i, and 10g databases.

You use this solution template to deploy a set of monitors that test the health, availability, and performance of an Oracle database. The deployed monitors will check general system statistics, such as cache hit ratios and disk I/O, and include tools that provide diagnostic information about important aspects of the database.

Usage Guidelines

Use the Oracle Database Solution to monitor statistics from Oracle 8i, 9i, 10g databases. Important system metrics are computed with data retrieved from system tables in the Oracle database. A wide range of Oracle system tables such as V$SYSSTAT, V$LATCH, V$ROLL_STAT, and V$BUFFER_POOL_STATISTICS are consulted to produce these metrics. In this way, the Oracle Database Solution implements the equivalent of many of the system monitoring scripts that come bundled with the Oracle installation.

Before configuring the Oracle Database Solution for deployment, you can consult the documentation for the Database Counter Monitor and the Log File Monitor for information about some of the prerequisites and parameters required by the solution template. For example, you will find more information on installing the Oracle JDBC driver needed to communicate with the database and the format of the log file path name parameter.

To deploy an Oracle Database Solution Template:

1. Click on the SiteScope container into which you want to add the Oracle Database Solution and expand the container to display the group containers.
2. Right-click the Oracle Database Solution template icon to display the action menu and select **Copy**.
3. Select the SiteScope container or the monitor group container into which you want to deploy the Oracle Database Solution.
4. Right-click on the container to display the action menu and select **Paste**. The Oracle Database Solution Variable Values form opens in the contents panel.
5. Complete the items on the Oracle Database Solution Variable Values form as described in the section "Oracle Database Solution Template Settings" below. When the required items are completed, click the **OK** button.
6. As SiteScope creates the monitors, a paste results message is shown listing the names of the monitors created along with messages indicating success or error. After the monitors have been created, select **Close**.

Note: Errors detected during the creation of monitors using a solution template are independent of the status returned when the individual monitors are run. This means that the monitors may be created successfully but that the configuration settings may be incorrect or that the system being monitored is unavailable.

Note: Solution Templates do not configure any automated alerts for the monitors created. You must create and associate one or more alert definitions to the monitors or monitor groups created by solution templates.

Oracle Database Solution Template Settings

Database Connection URL:

Enter the connection URL to the database you want to monitor. For example, jdbc:oracle:thin:@192.168.0.50:1521:ORCL.

Database User Name

Enter the user name that SiteScope should use to connect to the database.

Database Password

Enter the password for the user name that SiteScope should use to connect to the database.

Monitor Frequency

The frequency in seconds at which you'd like the deployed monitors to run. It is generally a good idea to enter a conservative frequency (10 minutes or greater) when first deploying the solution because some of the SQL queries invoked by the deployed monitors could impose some overhead on the database. Once the monitors are deployed, you will be able to edit the monitors individually and increase the frequencies on specific monitors, if necessary.

Connection Timeout

Enter a timeout value, in seconds, that the monitor should wait for a database connection.

Note: The sum of the Connection Timeout value and Query Timeout value should always be less than the Update every value for the monitor.

Query Timeout

Enter a timeout value, in seconds, that the monitor should wait for a database query to return results.

Note: The sum of the Connection Timeout value and Query Timeout value should always be less than the Update every value for the monitor.

Server

Choose the server you want to monitor. Click the choose server link to open the server selection screen. Select a server from the drop-down menu or enter an UNC path for the server you want to monitor.

Oracle Alert Log Path

Enter the full path to the Oracle alert log. Consult your database administrator or the Oracle documentation for information on how to access this file.

Oracle Listener Log Path

Enter the full path to the Oracle listener log. Consult your database administrator or the Oracle documentation for information on how to access this file.

Oracle Database Solution Tools

The Oracle Solution Template deploys several tools that you can use to gather diagnostic information about an Oracle database. These tools are deployed to the same group as the monitors that are deployed by the solution template. They are displayed in much the same way as monitors but they are set as disabled. These tools are identified by the bold text "Solution Tool" in the Status field of the group content table. See the section "Understanding Oracle Database Solution Tools" for more information.

When the user clicks on one of these Solution Tools, SiteScope will make a custom SQL query to the database via the Database Connection Test tool. The results of the query are found in a table at the bottom of the page. From this page, the tool may be run as many times as necessary by clicking the Connect and Execute Query button. Bear in mind that some tools may incur substantial overhead on the database, so executing them in quick succession may not be a good idea.

Understanding Oracle Database Solution Tools

The Oracle Database Solution Tools are preconfigured diagnostic tool actions that are associated with and accessible to a particular Oracle Database Solution template deployment. These tools are deployed into the same group as the monitors that are deployed by the Oracle Database Solution template. The tools are listed in the monitor detail table and identified with the name **Solution Tool** in the **Status** field of the table.

Although the Solution tools are listed in the monitor table, they are not monitor instances. They do not run automatically, display a status based on action results, or trigger alerts. They are preconfigured actions that make use of a SiteScope Diagnostic Tool to check certain statistics from the Oracle database that may indicate a performance problem.The following describes tools deployed as part of the Oracle Database Solution:

Tool Name	Description and Usage Guidelines
Oracle Solution Tool: Top Ten SQL Statements in Logical IOs Per Row	This tool performs a query which is designed to locate the most resource-intensive SQL statements being executed in the database. The V$SQL table is queried for the ten SQL statements which are performing the most logical IOs per row are displayed in a table. The statement IDs of these ten statements are displayed in a table, along with some additional resource-usage data for each statement. This additional data includes: Physical IO Blocks : the number of disk reads performed on behalf of the statement. Logical IOs : the number of buffer gets performed on behalf of the statement. Rows Processed : the number of rows processed when executing the statement. Logical IOs Per Row : the number of buffer gets performed per row that was processed when executing the statement. Runs : the number of executions of the statement. Logical IOs Per Run : the number of buffer gets per statement execution. **Note:** The action performed can have a significant impact on database resources and should not be executed frequently.
Oracle Solution Tool: No. of Sessions Waiting Per Event	This tool can be used in troubleshooting stuck sessions. When several sessions become unresponsive, this tool can determine whether the stuck sessions are all waiting on the same event. The tool action displays a table containing the number of sessions waiting on specific events.

Oracle Solution Tool: Shared Server Process Contention (Common Queue Average Wait Time)	This tool calculates the average wait time of the shared server message queue (the Common Queue as recorded in V$QUEUE). A high average wait time may indicate contention between shared server processes.
Oracle Solution Tool: Tablespaces With Less Than 2 Extents Available	This tool can be used to locate tablespaces which do not have enough adjacent free space to throw more than two new extents. Important: This tool will not be useful on all Oracle configurations. For example, the query used by this tool (see below) would not work correctly on a database that uses dictionary-managed tablespaces (DMTs). Even for databases that used locally-managed tablespaces (LMTs), the query may not apply, depending on the segment space management scheme used for a specific tablespace. Tablespace management is a very complex subject. If there is any doubt as to the applicability of this tool to your specific Oracle installation, the best course of action is to consult your local DBA and ask them about the usefulness of the query used by this tool with respect to the target database configuration. The following query is executed by this tool: SELECT owner, s.tablespace_name, segment_name, s.bytes, next_extent, MAX(f.bytes) largest FROM dba_segments s, dba_free_space f WHERE s.tablespace_name = f.tablespace_name(+) GROUP BY owner,s.tablespace_name,segment_name, s.bytes,next_extent HAVING next_extent*2>max(f.bytes)

You use the following steps to run or execute the Oracle Database Solution tools.

To run an Oracle Database Solution tool:

1 Click the group name for the group where the Oracle Solution monitors are deployed. The group detail page opens.

2. Find the Solution Tool for the action that you want to execute. See the **Name** column for the Solution Tool for a description of the action performed by that tool.
3. Click the **Tools** link to the right of the tool **Name** to execute the action. The Database Connection Test page opens. From this page, the tool may be run as many times as necessary by clicking the **Connect and Execute Query** button.

Note: Some Solution Tools may create significant overhead on the database depending on the query. Executing the tools in quick succession is therefore not advised.

The upper portion of the Database Connection Test page displays the database connection parameters used for the test. The results of the tool query are found in a table near the bottom of the page. Review the results based on the Description and Usage Guidelines for that tool.

9

SAP Solution Templates

To address the needs of SAP performance monitoring, Mercury offers SAP solution templates. The SiteScope SAP solution templates provide efficient and thorough monitoring of performance, availability, and usage statistics for SAP system components.

This chapter describes:	On page:
About the SAP Solution	107
Using the SAP R/3 Solution Template	108
Using the SAP J2EE Solution Template	111

About the SAP Solution

The SAP solution includes solution templates for the monitoring the following key SAP components:

- SAP CCMS
- SAP Java Web Application Server

The SAP Solution uses two solution templates which you use to deploy a collection of monitors configured with metrics to report on availability and performance. These monitoring configurations have been researched using best practice data and expertise from various sources.

Note: You must have the applicable SiteScope option license to use the SAP R/3 and SAP J2EE solution templates. Contact your Mercury sales representative for more information about licensing for solution templates.

The purpose of a solution template is to provide comprehensive SAP monitoring without requiring the SiteScope user or the IT organization to be experts on the application.

Benefits of the SAP Solution templates include:

- Reduces the need for SAP server monitoring and performance domain expertise
- Reduces the time to configure and deploy multi-level monitoring for SAP servers
- Helps identify both real-time performance bottlenecks and longer term trends

You use the SAP R/3 solution template to deploy monitoring for SAP R/3 systems. You use the SAP J2EE template to monitor the SAP Java Web Application server if this component is deployed in the IT environment.

Using the SAP R/3 Solution Template

The SiteScope SAP R/3 solution template provides the tools you use to monitor the availability, usage statistics, and server performance statistics for SAP R/3 systems. This solution template deploys a set of monitors that test the health, availability, and performance of SAP R/3 servers.

System Requirements

Before you can use the SAP R/3 solution template, there are a number of configuration requirements involving the server environment. The following lists an overview of these requirements:

- SAP Java Connector libraries should be copied to the appropriate SiteScope folders.

➤ You need to know the user name and password that SiteScope must use to log into the SAP R/3 server.

For more information on system and configuration requirements, see "SAP CCMS Monitor" on page 945. This monitor is deployed as part of the SAP R/3 solution template.

Deploying the SAP R/3 Solution Template

You use the following steps to deploy the SAP R/3 solution template.

To deploy the SAP R/3 Solution Template:

1. Click on the SiteScope container into which you want to add the SAP Solution and expand the container to display the group containers.
2. Right-click the SAP R/3 solution template icon to display the action menu and select **Copy**.
3. Select the SiteScope container or the monitor group container into which you want to deploy the SAP R/3 solution.
4. Right-click on the container to display the action menu and select **Paste**. The Variable Values form opens in the contents panel.
5. Complete the items on the SAP Solution Variable Values form as described in the section "SAP R/3 Solution Template Settings" below. When the required items are completed, click **OK**.
6. As SiteScope creates the monitors, a paste results message is shown listing the names of the monitors created along with messages indicating success or error. After the monitors have been created, click **Close**.

Note: Errors detected during the creation of monitors using a solution template are independent of the status returned when the individual monitors are run. This means that the monitors may be created successfully but that the configuration settings may be incorrect or that the system being monitored is unavailable.

After deploying the monitors, you should review the Error and Warning status thresholds and adjust them according to the importance of the monitored element. You should also create alerts and associate them to the newly created monitors to provide notification when an error is detected.

Note: Solution templates do not configure any automated alerts for the monitors created. You must create and associate one or more alert definitions to the monitors or monitor groups created by solution templates.

SAP R/3 Solution Template Settings

The following describes the settings for the SAP R/3 solution:

Application Server

Enter the address of the SAP server you want to monitor.

SAP Client

Enter the Client to use for connecting to SAP.

System Number

Enter the System number for the SAP server.

Authentication User Name

Enter the user name required to connect to the SAP server.

Authentication Password

Enter the password required to connect to the SAP server.

Router String (Optional)

If you are connecting through a router, enter a router address string. You can locate the router address using the SAP Logon tool from the SAP Client software. Open the Logon console, select the server you want to monitor, and select **Properties** to view the router address. If you are not connecting through a router, leave this field blank.

Using the SAP J2EE Solution Template

The SiteScope SAP J2EE solution enables you to monitor the availability and server statistics for SAP Java Web application server clusters.

This solution template deploys a monitor that tests the health, availability, and performance of SAP Java Web application servers. You can use this solution template to deploy monitors for server-wide resources and metrics.

System Requirements

Before you can use the SAP J2EE solution template, there are a number of configuration requirements involving the server environment. The following lists an overview of these requirements:

- SAP Java Web application server libraries must be copied to the appropriate SiteScope folders.
- You must know the user name and password that SiteScope must use to log into the SAP Java Web application server.

For more information on system and configuration requirements, see "SAP Java Web Application Server Monitor" on page 967. This monitor is deployed as part of the SAP J2EE solution template.

Deploying the SAP J2EE Solution Template

You use the following steps to deploy the SAP J2EE solution template.

To deploy a SAP J2EE solution template:

1. Click the SiteScope container into which you want to add the SAP J2EE solution template and expand the container to display the group containers.
2. Right-click the SAP J2EE solution template icon to display the action menu and select **Copy**.
3. Select the SiteScope container or the monitor group container into which you want to deploy the SAP J2EE solution template.
4. Right-click on the container to display the action menu and select **Paste**. The Variable Values page opens in the contents panel.

5 Complete the items on the SAP Solution Variable Values page as described in the section "SAP J2EE Solution Template Settings" below. When the required items are completed, click the **OK** button.

6 As SiteScope creates the monitors, a paste results message is shown listing the names of the monitors created along with messages indicating success or error. After the monitors have been created, click **Close**.

Note: Errors detected during the creation of monitors using a solution template are independent of the status returned when the individual monitors are run. This means that the monitors may be created successfully but that the configuration settings may be incorrect or that the system being monitored is unavailable.

After the monitors have been created, you can select the **Return** link to return to the group detail page to view the status of the monitors.

After deploying the monitors, you should review the Error and Warning status thresholds and adjust them according to the importance of the monitored element. You should also create alerts and associate them to the newly created monitors to provide notification when an error is detected.

Note: Solution Templates do not configure any automated alerts for the monitors created. You must create and associate one or more alert definitions to the monitors or monitor groups created by solution templates.

SAP J2EE Solution Template Settings

The following describes the settings for the SAP J2EE Solution Template:

Application Server

Enter the address of the SAP Java Web Application Server you want to monitor.

Port

Enter the port number to use for connecting to the SAP server. The default port of 50004 is typically used.

Authentication User Name

Enter the user name required to connect to the SAP server.

Authentication Password

Enter the password required to connect to the SAP server.

10

Siebel Solution Templates

To address the needs of Siebel performance monitoring, Mercury Interactive offers Siebel Solutions. The SiteScope Siebel Solution templates provide efficient and thorough monitoring of performance, availability, and usage statistics for Siebel Application Server installed on Microsoft Windows operating systems.

This chapter describes:	On page:
About the Siebel Solution	115
Using the Siebel Application Server Solution Template	116
Using the Siebel Gateway Server Solution Template	122
Using the Siebel Web Server Solution Template	124

About the Siebel Solution

The Siebel Solution includes solution templates for the monitoring the following key Siebel components:

- Siebel Application Server
- Siebel Gateway Server
- Siebel Web Server

The Siebel Solution uses three solution templates which you use to deploy a collection of monitors configured with metrics to report on availability and performance. These monitoring configurations have been researched using best practice data and expertise from various sources.

Note: You must have the applicable SiteScope option license to use the Siebel Solution templates. Contact your Mercury sales representative for more information about Solution licensing.

The Siebel Solution templates can be deployed to monitor only those Siebel application servers that are installed on Microsoft Windows operating system and not Unix or other operating systems.

The purpose of a solution template is to provide comprehensive Siebel monitoring without requiring the SiteScope user or the IT organization to be experts on the application.

Benefits of the Siebel Solution templates include:

- Reduces the need for Siebel server monitoring and performance domain expertise
- Reduces the time to configure and deploy multi-level monitoring for Siebel servers
- Helps identify both real-time performance bottlenecks and longer term trends

The primary solution template for Siebel is the Siebel Application Server template. This solution template is applicable to all Siebel deployments on Windows platforms. You use this template to deploy monitoring for the core of the Siebel application. You use the Siebel Gateway Server and Siebel Web Server templates if these optional components are deployed in the IT environment.

Using the Siebel Application Server Solution Template

The SiteScope Siebel Application Server Solution Template provides tools you use to monitor the availability, usage statistics, and server performance statistics for Siebel Application servers installed on Windows platforms. This solution template will deploy a set of monitors that test the health, availability, and performance of Siebel Application Servers.

System Requirements

Before you can use the Siebel Application Server Solution Template, there are a number of configuration requirements involving the server environment. The following lists an overview of these requirements:

- The Siebel Server Manager client must be installed on the machine where SiteScope is running or accessible to the SiteScope machine. There are several options for how you can do this. See the documentation for the Siebel Server Manager Monitor for more information.
- You will need to know the install path for the Server Manager client to be able to setup Siebel Server Manager monitors in SiteScope. If the client is installed on the machine where SiteScope is running, this will be the path on that machine. If the client is installed on a remote machine, you need to know the fully qualified path to the client executable relative to that machine.
- You need to know the name of the Siebel application(s) that are available in your network. For example, call center, sales, and so forth.
- You need to install and configure an ODBC System DSN name that can be used for monitoring Siebel database tables.
- You need to know the user and password that SiteScope will use for logging into the Siebel server. This user must be granted Siebel Administrator responsibility on the Siebel server.
- You need to know a significant list of Siebel system component names and their corresponding aliases. See the section on the Settings in the Siebel Application Server Solution Form for a listing of component names and aliases.

See the sections on the "Siebel Application Server Monitor" and "Database Query Monitor" for more information on system and configuration requirements. These monitor types that are deployed as part of the Siebel Application Server Solution Template.

Deploying the Siebel Application Server Solution Template

You use the following steps to deploy the Siebel Application Server Solution Form.

To deploy the Siebel Application Server Solution Template:

1. Click on the SiteScope container into which you want to add the Siebel Solution and expand the container to display the group containers.
2. Right-click the Siebel Application Server Solution template icon to display the action menu and select **Copy**.
3. Select the SiteScope container or the monitor group container into which you want to deploy the Siebel Application Server Solution.
4. Right-click on the container to display the action menu and select **Paste**. The Variable Values form opens in the contents panel.
5. Complete the items on the Siebel Solution Variable Values form as described in the section "Siebel Application Server Solution Template Settings" below. When the required items are completed, click the **OK** button.
6. As SiteScope creates the monitors, a paste results message is shown listing the names of the monitors created along with messages indicating success or error. After the monitors have been created, select **Close**.

Note: Errors detected during the creation of monitors using a solution template are independent of the status returned when the individual monitors are run. This means that the monitors may be created successfully but that the configuration settings may be incorrect or that the system being monitored is unavailable.

After the monitors have been created, you can select the Return link to return the group detail page to view the status of the monitors.

After deploying the monitors, you should review the Error and Warning status thresholds and adjust them according to the importance of the monitored element. You should also create alerts and associate them to the newly created monitors to provide notification when an error is detected.

Note: Solution Templates do not configure any automated alerts for the monitors created. You must create and associate one or more alert definitions to the monitors or monitor groups created by solution templates.

Siebel Application Server Solution Template Settings

The following describes the settings for the Siebel Application Server Solution:

Server

Select the machine name for the server where Siebel Application Server is running. Use the choose server to view the server selection screen. Use the Server drop-down menu to select the server where the Siebel Application Server is running.

Enterprise

Enter the Siebel Enterprise server name.

Gateway

Enter the name of the Siebel Gateway server machine.

Server Logical Instance Name

Enter the Siebel server logical name.

Username

Enter the Siebel Client user name.

Password

Enter the password for the Siebel Client.

Srvrmgr Script Path

Enter the local path to the Siebel server manager client. For example: D:\sea703\client\bin.

Siebel Disk

Enter the disk name where Siebel is installed.

Siebel Root Dir

Enter the path of the shared Siebel root directory. For example, the shared root directory for a Siebel 7.5.2 server would be: `sea752`.

Siebel ODBC Name

Enter the local ODBC name that SiteScope should use for accessing the Siebel database.

DB Username

Enter the username SiteScope should use to access the Siebel database.

DB Password

Enter the password for the username used to access the Siebel database.

CG Callcenter Name

Enter the Siebel CallCenter component group name.

CG Callcenter Alias

Enter the Siebel CallCenter component group alias.

CG System Management Name

Enter the Siebel System Management component group name.

CG System Management Alias

Enter the Siebel System Management component group alias.

CP Callcenter Name

Enter the Siebel CallCenter component name.

CP Callcenter Alias

Enter the Siebel CallCenter component alias.

CP eService Name

Enter the Siebel eService component name.

CP eService Alias

Enter the Siebel eService component alias.

CP Srvr Request Broker Name

Enter the Siebel Server Request Broker component name.

CP Srvr Request Broker Alias

Enter the Siebel Server Request Broker component alias.

CP_Srvr_Request_Processor_Name

Enter the Siebel Server Request Processor component name.

CP Srvr Request Processor Alias

Enter the Siebel Server Request Processor component alias.

CP Server Manager Name

Enter the Siebel Server Manager component name.

CP Server Manager Alias

Enter the Siebel Server Manager component alias.

CP File System Manager Name

Enter the Siebel File System Manager component name.

CP File System Manager Alias

Enter the Siebel File System Manager component alias.

CP Client Administration Name

Enter the Siebel Client Administration component name.

CP Client Administration Alias

Enter the Siebel Client Administration component alias.

Using the Siebel Gateway Server Solution Template

The SiteScope Siebel Gateway Server Solution allows you to monitor the availability and server statistics for Siebel Gateway servers installed on Windows platforms.

This solution template will deploy a set of monitors that test the health, availability, and performance of Siebel Gateway Servers. You can use this solution template to deploy monitors for server-wide resources and metrics.

Deploying the Siebel Gateway Server Solution Template

You use the following steps to deploy the Siebel Gateway Server Solution Template.

To deploy a Siebel Gateway Server Solution Template:

1. Click on the SiteScope container into which you want to add the Siebel Solution and expand the container to display the group containers.
2. Right-click the Siebel Gateway Server Solution template icon to display the action menu and select **Copy**.
3. Select the SiteScope container or the monitor group container into which you want to deploy the Siebel Gateway Server Solution.
4. Right-click on the container to display the action menu and select **Paste**. The Variable Values form opens in the contents panel.
5. Complete the items on the Siebel Solution Variable Values form as described in the section “Siebel Gateway Server Solution Template Settings” below. When the required items are completed, click the **OK** button.
6. As SiteScope creates the monitors, a paste results message is shown listing the names of the monitors created along with messages indicating success or error. After the monitors have been created, select **Close**.

   As the monitors are created, the monitor type and name are displayed along with messages of any errors found. A "success" message is shown if the monitors are created successfully. The process does not run the monitor.

Note: Errors detected during the creation of monitors using a solution template are independent of the status returned when the individual monitors are run. This means that the monitors may be created successfully but that the configuration settings may be incorrect or that the system being monitored is unavailable.

After the monitors have been created, you can select the Return link to return the group detail page to view the status of the monitors.

After deploying the monitors, you should review the Error and Warning status thresholds and adjust them according to the importance of the monitored element. You should also create alerts and associate them to the newly created monitors to provide notification when an error is detected.

Note: Solution Templates do not configure any automated alerts for the monitors created. You must create and associate one or more alert definitions to the monitors or monitor groups created by solution templates.

Siebel Gateway Server Solution Template Settings

The following describes the settings for the Siebel Gateway Server Solution:

Server

Enter the name of the server where the Siebel Gateway Server is running. Do NOT enter backslashes (\\) that indicate a UNC path as part of the name of the server.

Siebel Disk

Enter the disk drive where the Siebel gateway server is running.

Siebel Directory

Enter the path to the Siebel Directory. This directory should contain at least an Admin Console installation.

Using the Siebel Web Server Solution Template

The SiteScope Siebel Web Server Solution allows you to monitor the availability and server statistics for Siebel Web servers installed on Windows platforms. This solution template will deploy a set of monitors that test the health, availability, and performance of Siebel Web Servers.

System Requirements

Before you can use the Siebel Solution, there are a number of configuration requirements involving the server environment:

- SiteScope server must be able to connect to the machine where the Siebel Web Server is running.
- Siebel Web Server Solution is designed for use with Siebel running on Microsoft Windows platforms.
- Template assumes that the Siebel Web Server is running on Microsoft Internet Information Server (IIS).

Deploying the Siebel Web Server Solution Template

You use the following steps to deploy the Siebel Web Server Solution Template.

To deploy a Siebel Web Server Solution Template:

1. Click on the SiteScope container into which you want to add the Siebel Solution and expand the container to display the group containers.
2. Right-click the Siebel Web Server Solution template icon to display the action menu and select **Copy**.
3. Select the SiteScope container or the monitor group container into which you want to deploy the Siebel Web Server Solution.

4 Right-click on the container to display the action menu and select **Paste**. The Variable Values form opens in the contents panel.

5 Complete the items on the Siebel Solution Variable Values form as described in the section "Siebel Web Server Solution Template Settings" below. When the required items are completed, click the **OK** button.

6 As SiteScope creates the monitors, a paste results message is shown listing the names of the monitors created along with messages indicating success or error. After the monitors have been created, select **Close**.

After deploying the monitors, you should review the Error and Warning status thresholds and adjust them according to the importance of the monitored element. You should also create alerts and associate them to the newly created monitors to provide notification when an error is detected.

Note: Solution Templates do not configure any automated alerts for the monitors created. You must create and associate one or more alert definitions to the monitors or monitor groups created by solution templates.

Siebel Web Server Solution Template Settings

The following describes the settings on the Siebel Web Server Solution Form:

Server

Select the Siebel Web server machine name. Use the choose server to view the server selection screen. Use the Server drop-down menu to select the server where the Siebel Web server is running.

Siebel Root Dir

Enter the name of the shared Siebel root directory. For example: sea752.

Siebel Disk

Enter the disk name or drive letter where the Siebel Web server is installed.

Application

Enter the Siebel application to monitor. For example: callcenter_enu. Consult with your Siebel administrator for information on names of the installed Siebel applications.

Username

Enter the Siebel Client user name needed to log into the Siebel Web server.

Password

Enter the Siebel Client password needed to log into the Siebel Web server.

11

WebLogic Solution Template

To address the needs of WebLogic performance monitoring, Mercury Interactive offers the WebLogic Solution. The SiteScope WebLogic Solution template provides efficient and thorough monitoring of performance, availability, and usage statistics for BEA WebLogic Server 6.x, 7.x and 8.x application servers.

This chapter describes:	On page:
Understanding the WebLogic Solution	127
Using the WebLogic Solution Template	129

Understanding the WebLogic Solution

This solution uses a template which you can use to deploy a collection of WebLogic Monitors configured with default metrics. These monitoring configurations have been researched using best practice data and expertise from various sources. The WebLogic Solution monitor deployment process is highly customizable in that it allows the user to select the specific J2EE components on an application server which SiteScope should actively monitor.

Note: You must have the applicable SiteScope option license to use the WebLogic Solution Template. Contact your Mercury sales representative for more information about Solution licensing.

The purpose of a solution template is to provide comprehensive WebLogic monitoring without requiring the SiteScope user or the IT organization to be experts on the application. An in-depth description of the WebLogic Solutions is available as a separate document as part of the SiteScope installation. This document can be found at **<SiteScope root directory>\sisdocs\pdfs\Sitescope_WebLogic_Best_Practices.pdf**.

Note: This is a password protected document. The password is provided along with the WebLogic Solution license key from Mercury.

Benefits of the WebLogic Solution Template include:

- Reduces the need for WebLogic performance domain expertise
- Reduces the time to configure and deploy WebLogic monitors
- Helps identify both real-time performance bottlenecks and longer term trends
- Adds no overhead to production systems

The WebLogic Solution Template deploys monitors that target the following aspects of WebLogic performance and health:

Server Performance Statistics

This category refers to a collection of server-wide resources that are exposed through the management interface of a WebLogic Application Server. Examples of these server-wide resources include:

- JVM Runtime
- JTA Runtime
- Thread Pools
- JDBC Pools

Application Performance Statistics

Metrics for all of your deployed applications, EJBs, web applications, and servlets are available for monitoring through the WebLogic Solution. The user is responsible for selecting which of these J2EE components he would like to have monitors automatically deployed for. A set of metrics based on WebLogic best practices are monitored for each selected J2EE component. Some of the J2EE components that can be monitored through this solution include:

- Web Applications
- Servlets
- General EJB Component Statistics
- EJB Transaction Statistics
- EJB Pool Statistics
- EJB Cache Statistics

Using the WebLogic Solution Template

The SiteScope WebLogic Solution facilitates the implementation of best-practice monitoring of WebLogic Application Servers with a minimum of configuration. This solution applies to WebLogic Application Server versions 6.x, 7.x, and 8.x.

This solution template will deploy a set of monitors that test the health, availability, and performance of a WebLogic Application Server and its deployed applications and components. The deployed monitors will monitor server-wide statistics, such as memory usage, as well as metrics specific to individual J2EE components, such as the number of activates and passivates of a particular EJB.

Usage Guidelines

Use the WebLogic Solution to monitor statistics from WebLogic 6.x, 7.x, and 8.x servers. This solution will automatically create several groups by default which monitor important application server metrics, but it also provides a user interface which allows you, the user, to select all or some of the many individual components that are available for monitoring.

The WebLogic Solution Template deploys a WebLogic Application Server Monitor for each module that is selected from the user interface. This monitor uses the Java JMX interface to access Runtime MBeans on the WebLogic server. An MBean is a container that holds the performance metrics. You may need to set certain permissions on the WebLogic server for SiteScope to be able to monitor MBeans. For an overview on configuring access to WebLogic servers for SiteScope monitors, see the section "WebLogic Application Server Monitor".

Deploying the WebLogic Solution Template

You use the following steps to deploy the WebLogic Application Server Solution Form.

To deploy a WebLogic Solution Template:

1. Click on the SiteScope container into which you want to add the WebLogic Solution and expand the container to display the group containers.
2. Right-click the WebLogic Solution template icon to display the action menu and select **Copy**.
3. Select the SiteScope container or the monitor group container into which you want to deploy the WebLogic Solution.
4. Right-click on the container to display the action menu and select **Paste**. The Variable Values form opens in the contents panel.
5. Complete the items on the WebLogic Solution Variable Values form as described in the section "WebLogic Solution Template Settings" below. When the required items are completed, click the **OK** button.
6. As SiteScope creates the monitors, a paste results message is shown listing the names of the monitors created along with messages indicating success or error. After the monitors have been created, select **Close**.

Note: Errors detected during the creation of monitors using a solution template are independent of the status returned when the individual monitors are run. This means that the monitors may be created successfully but that the configuration settings may be incorrect or that the system being monitored is unavailable.

After the monitors have been created, you can select the Return link to return the group detail page to view the status of the monitors.

After deploying the monitors, you should review the Error and Warning status thresholds and adjust them according to the importance of the monitored element. You should also create alerts and associate them to the newly created monitors to provide notification when an error is detected.

Note: Solution Templates do not configure any automated alerts for the monitors created. You must create and associate one or more alert definitions to the monitors or monitor groups created by solution templates.

WebLogic Solution Template Settings

The following describes the settings for the WebLogic Application Server Solution:

Server

Enter the name or address of the server where WebLogic is running.

Port Number

Enter the port number that the WebLogic server is responding on. The default port is 7001.

User Name

Enter the username required to log into the WebLogic server.

Password

Enter the password required to log into the WebLogic server.

WebLogic Jar File

Enter the absolute path name to the weblogic.jar file on the SiteScope machine. This file must be installed on the SiteScope server and can be downloaded from the WebLogic server. An example path is: c:\bea\weblogic7\ebcc\lib\ext\weblogic.jar. This file is not strictly required for monitoring some earlier versions of WebLogic 6. In this case, leaving this box blank will normally cause any necessary classes to be downloaded directly from the WebLogic server. Note that this is not as efficient as loading the classes from the a *.jar file on the server where SiteScope is running.

Note: Do not install the weblogic.jar file in the SiteScope directory tree. For example, do not install it in the <SiteScope install path>/SiteScope/java/lib/ext directory as this will cause the WebLogic monitors to fail. You must create a separate directory on the server where SiteScope is running for this file.

Secure Server

Check this box if you are using a secure server connection option. Note: If you select this option, you must enter the applicable port number used by the WebLogic server for secure connections. The default secure server port is 7002.

You must enter valid connection parameters before clicking the Show Applications button. When the correct connection information is supplied, SiteScope uses this to query the server and populate a hierarchical list of the selectable modules that you may monitor. Selecting a module will cause a monitor to be deployed against it. The metrics for each monitor are automatically created according to the type of module that is being monitored.

Selecting Modules for Monitoring

The WebLogic Solution presents a hierarchical list from which the user can select the modules to deploy WebLogic Monitors against. This list is broken down into two main sections:

- per-server resources
- J2EE components organized by application

Some of the modules in these categories are automatically selected by default because they represent critical components in the system (for example, the JVM statistics for the application server). The remainder of the modules are not automatically selected. This allows the user to customize the deployment of this solution in order to focus on one application, a particular type of EJB, a set of servlets and web applications, or some other aspect of the application server.

For the most part, the organization of this list of modules is intuitive. The hierarchy of applications, EJBs, web applications, and servlets is very similar to the organization of these entities in the WebLogic Administration Console. In almost every case, selecting a module will cause a monitor with all relevant metrics to be deployed against that part of the WebLogic server. However, when selecting EJBs to monitor, you will notice that they are broken down according to three types of metrics: Pool, Transaction, and Cache. The reason for this is twofold: (1) it is more useful to be able to monitor one aspect of a particular EJB instead per WebLogic Monitor for purposes of alerting and organization, and (2) not all three of these types of metrics are available for all EJBs. Below is a brief description of the metrics that are monitored for each type of EJB monitoring:

- Per-EJB Transaction Statistics This category of EJB monitor contains metrics related to transactions made for the EJB. These metrics include the number transactions rolled back, the number of transactions which timed out, and the number of transactions that were successfully committed.

- Per-EJB Pool Statistics This category of EJB monitor contains metrics related to the pool for the EJB. When the user selects an EJB under this heading, many useful metrics are monitored, including the number of times an attempt to get a bean instance from the pool failed, the number of current available instances in the pool, the number of threads currently waiting for an instance, and the number of times a bean instance was destroyed due to a non-application Exception.
- Per-EJB Cache Statistics The cache statistics include any metrics relating to the caching of the particular EJB. Metrics like the number of cache hits and misses, and the number of activates and passivates of the EJB are monitored when an EJB under this heading is selected for monitoring.

When you have finished making your module selections in the popup window, scroll to the bottom of the Module Selection window and click the Select Modules button. This will update the main browser window with a list of the modules you selected. You can then review your selections and remove any modules that you don't want a monitor to be created for.

When you are satisfied with the list of selected modules in the main browser window, you may hit the Submit button to proceed to the next step in deploying the WebLogic Solution.

12

WebSphere Solution Template

To address the needs of WebSphere performance monitoring, Mercury Interactive offers the WebSphere Solution. The SiteScope WebSphere Solution provides efficient and thorough monitoring of performance, availability, and usage statistics for IBM WebSphere Server 5.x application servers.

This chapter describes:	On page:
Understanding the WebSphere Solution	135
Using the WebSphere Solution Template	137

Understanding the WebSphere Solution

This solution uses a template you can use to deploy a collection of WebSphere Monitors configured with default metrics. These monitoring configurations have been researched using best practice data and expertise from various sources. The WebSphere Solution monitor deployment process is highly customizable in that it allows the user to select the specific J2EE components on an application server which SiteScope should actively monitor.

Note: You must have the applicable SiteScope option license to use the WebSphere Solution templates. Contact your Mercury sales representative for more information about Solution licensing.

The purpose of a solution template is to provide comprehensive WebSphere monitoring without requiring the SiteScope user or the IT organization to be experts on the application. An in-depth description of the WebSphere Solutions is available as a separate document as part of the SiteScope installation. This document can be found at **<SiteScope root directory>\sisdocs\pdfs\SiteScope_WebSphere_Best_Practices.pdf**.

Note: This is a password protected document. The password is provided along with the WebSphere Solution license key from Mercury.

Benefits of the WebSphere solution template include:

- Reduces the need for WebSphere performance domain expertise
- Reduces the time to configure and deploy WebSphere monitors
- Helps identify both real-time performance bottlenecks and longer term trends
- Adds no overhead to production systems

The WebSphere Solution Template deploys monitors that target the following aspects of WebSphere performance and health:

Server Performance Statistics

This category refers to a collection of server-wide resources that are exposed through the management interface of a WebSphere Application Server. Examples of these server-wide resources include:

- JVM Runtime
- The Transaction Manager
- Thread Pools
- The Servlet Session Manager

Application Performance Statistics

Metrics for all of your deployed applications, EJBs, web applications, and servlets are available for monitoring through the WebSphere Solution. The user is responsible for selecting which of these J2EE components he would like to have monitors automatically deployed for. A set of metrics based on WebSphere best practices are monitored for each selected J2EE component. Some of the J2EE components that can be monitored through this solution include:

- Web Applications
- Servlets
- EJB Components
- Entity EJB Statistics
- Stateful Session EJB Statistics
- Stateless Session EJB Statistics

Using the WebSphere Solution Template

The SiteScope WebSphere Application Server Solution allows you to monitor the availability, server statistics, and deployed J2EE components on a IBM WebSphere Application Server 5.x.

Usage Guidelines

This solution template will deploy a set of monitors that test the health, availability, and performance of IBM WebSphere 5.x Application Servers. It uses IBM's JMX interface to the Performance Monitoring Infrastructure of WebSphere. You can use this solution template to deploy monitors for server-wide resources and metrics (i.e. thread pool and JVM metrics). You can also create monitors for the deployed EJBs, Web Applications, and Servlets using this solution template. An in-depth description of the WebSphere Solution is available in a Best Practices document. For details, see “Understanding the WebSphere Solution” on page 135.

System Requirements

Before you can use the WebSphere Solution, there are a number of configuration requirements involving the server environment. For an overview of these requirements, see the section "WebSphere Application Server Monitor".

Deploying the WebSphere Solution Template

You use the following steps to deploy the WebSphere Application Server Solution.

To deploy a WebSphere Solution Template:

1. Click on the SiteScope container into which you want to add the WebSphere Solution and expand the container to display the group containers.
2. Right-click the WebSphere Solution template icon to display the action menu and select **Copy**.
3. Select the SiteScope container or the monitor group container into which you want to deploy the WebSphere Solution.
4. Right-click on the container to display the action menu and select **Paste**. The Variable Values form opens in the contents panel.
5. Complete the items on the WebSphere Solution Variable Values form as described in the section "WebSphere Solution Template Settings" below. When the required items are completed, click the **OK** button.
6. As SiteScope creates the monitors, a paste results message is shown listing the names of the monitors created along with messages indicating success or error. After the monitors have been created, select **Close**.

Note: Errors detected during the creation of monitors using a solution template are independent of the status returned when the individual monitors are run. This means that the monitors may be created successfully but that the configuration settings may be incorrect or that the system being monitored is unavailable.

After the monitors have been created, you can select the Return link to return the group detail page to view the status of the monitors.

After deploying the monitors, you should review the Error and Warning status thresholds and adjust them according to the importance of the monitored element. You should also create alerts and associate them to the newly created monitors to provide notification when an error is detected.

Note: Solution Templates do not configure any automated alerts for the monitors created. You must create and associate one or more alert definitions to the monitors or monitor groups created by solution templates.

WebSphere Solution Template Settings

The following describes the settings on the WebSphere Application Server Solution Form:

WebSphere Server

Enter the name of the server where the WebSphere Application is running. Do NOT enter backslashes (\\) that indicate a UNC path as part of the name of the server.

WebSphere Port Number

Enter the port number of WebSphere server. This should be the SOAP port for WebSphere 5.x+. The default port number is 8880.

WebSphere User Name

Enter the user name that SiteScope should use to login to WebSphere server.

WebSphere Password

Enter the password that SiteScope should use to login to WebSphere server.

WebSphere Directory

Enter the path to the WebSphere Directory. This directory should contain at least an Admin Console installation.

WebSphere Client Properties File

Enter the custom client properties file. For WebSphere 5.x+, you should select an appropriate soap.client.props file. By default the /properties/soap.client.props file will be used.

WebSphere Classpath

Enter any extra classpath elements needed for monitor program.

You must enter valid connection parameters before clicking the Show Applications button. When the correct connection information is supplied, SiteScope uses this to query the server and populate a hierarchical list of the selectable modules that you may monitor. Selecting a module will cause a monitor to be deployed against it. The metrics for each monitor are automatically created according to the type of module that is being monitored.

Part III

SiteScope Monitors

13

Apache Server Monitor

The Apache Server Monitor allows you to monitor the administrative and performance statistics for an Apache server.

This chapter describes:	On page:
About the Apache Server Monitor	143
Configuring the Apache Server Monitor	144

About the Apache Server Monitor

Use the Apache Server Monitor to monitor the content of server administration pages for Apache servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate monitor instance for each Apache server you are running.

Before you can use the Apache Server Monitor, you will need to configure the Apache server you want to monitor so that status reports (server-status) are enabled for the server. The steps needed to do this may vary depending on the version of Apache you are using.

You will also need to enable extended status (ExtendedStatus On) in the configuration file.

You will also need to know the URL of the server statistics page for the server you want to monitor. The SiteScope Apache Server Monitor currently supports the server status page available via http://*server_address:port*/server-status?auto. The port will normally be port 80 although this may vary depending on the server set up and your environment. For some Apaches server configurations you may need to use the server name rather than an IP address in order to access the server statistics page.

The default run schedule for this monitor is every 10 minutes, but you can change it to run more or less often using the **Frequency** setting.

Configuring the Apache Server Monitor

The Apache Server Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the Apache Server Monitor.

Main Settings for the Apache Server Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the Apache Web Server, how often this Apache Server Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this Apache Server monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the Apache Server Monitor should system check the Apache Web Server. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

URL

Choose the server URL you want to verify with this monitor. This should be the Apache server statistics URL which usually has the form of http://*servername:port*/server-status?auto.

Counters

Choose the server performance parameters or counters you want to check with this monitor. The table list to the right of this item displays those currently selected for this monitor. Click **Get Counters** to bring up the counters selection screen. Check or clear the check boxes on the Get Counters screen to select one or more counters to monitor on this server. The performance parameters or counters available for the Apache Server Monitor include:

- Total Accesses
- Total kBytes
- CPULoad (not available on most Win32 versions)
- Uptime
- ReqPerSec
- BytesPerSec
- BytesPerReq
- BusyWorkers
- IdleWorkers
- BusyServers
- IdleServers

Advanced Settings for the Apache Server Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Apache Server Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Timeout

The number of seconds that the monitor should wait for a response from the server before timing-out. Once this time period passes, the monitor will log an error and report an error status.

Server OS

Use this box to select the operating system that the Apache server is running under. The default is Unix. This is used to correctly read server statistics from Apache based on the operating system platform.

HTTP Proxy

Optionally, a proxy server can be used to access the server. Enter the domain name and port of an HTTP Proxy Server.

Authorization User Name

If the server you want to monitor requires a name and password for access, enter the name in this box.

Authorization Password

If the server you want to monitor requires a name and password for access, enter the password in this box.

NT Challenge Response

Check this box if you want SiteScope to use Window's NT Challenge Response authorization when accessing.

Proxy Server User Name

If the proxy server requires a name and password to access the server, enter the name here. Technical note: your proxy server must support Proxy-Authenticate for these options to function.

Proxy Server Password

If the proxy server requires a name and password to access the server, enter the password here. Technical note: your proxy server must support Proxy-Authenticate for these options to function.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule

➤ Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set one or more status thresholds criteria for each status condition per monitor instance. The status of the monitor and any associated alert action will be set based on comparison of all the threshold criteria you define for the monitor. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the Apache Server or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the Apache Server Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

14

ASP Server Monitor

The ASP (Active Server Pages) Monitor allows you to monitor the availability of an Microsoft ASP server on Windows NT systems. The error and warning thresholds for the monitor can be set on one or more ASP server performance statistics.

This chapter describes:	On page:
About the ASP Server Monitor	151
Configuring the ASP Server Monitor	152

About the ASP Server Monitor

Use the ASP Server Monitor to monitor the server performance parameters for Microsoft ASP servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate monitor instance for each ASP Server you are running.

The Remote Registry service must be running on the machine where the ASP server is running if the ASP Server is running on Windows 2000.

The ASP Server Monitor makes use of Performance Counters to measure application server performance. SiteScope will need to be running under an account that has the necessary administrative security privileges to access performance counter data from remote servers. If the servers you want to monitor are in a different domain, are governed under a different policy, or require a unique login different than the account SiteScope is running under, then you will need to define the connection to these servers under the NT Remote Preferences option in the SiteScope Preferences.

The default run schedule for this monitor is every 10 minutes, but you can change it to run more or less often using the **Frequency** setting.

Configuring the ASP Server Monitor

The ASP Server Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the ASP Server Monitor.

Main Settings for the ASP Server Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the ASP server, how often this ASP Server Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this ASP Server monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the ASP Server Monitor should system check the ASP server. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Server

Choose the server where the ASP Server you want to monitor is running. Use the drop-down list to select the server from the list of remote servers that are available to the SiteScope agent.

Counters

You use the features associated with the **Counters** setting to choose and manage the metrics you want to monitor with the ASP Server Monitor. Use the following steps to select and add counters.

To select or add counters:

1. Click **Get Counters** to query the remote system. After SiteScope has successfully connected to the remote system, the Get Counters selection dialogue opens.
2. Use the features in the Get Counters selection dialogue screen to select the ASP server metrics you want to monitor. Use the expandable menu controls as applicable to browse the available counters.
3. Use the check boxes to select between one and ten counters to be monitored.
4. Click **OK** to add the selected counters to the monitor configuration. The Get Counters selection dialogue closes and the monitor properties are updated with your selection.

Use the following steps to remove a counter from the selected counters list.

To remove or edit counters:

1. Click to edit the monitor for which you want to remove counters. Alternately, you may select the monitor you want to edit and click the Properties tab and click the **Edit** button. The monitor Properties screen opens.
2. Click the **Get Counters** button to open the Get Counters selection dialogue.
3. Clear the check box to the left of the current counter you want to remove.

   At this point, you may add other counters to the monitor by clicking the applicable check boxes.
4. Click **OK** at the bottom of the screen to update the monitor.

The performance parameters or counters available for the ASP Server Monitor include, but are not limited to:

- Errors/Sec
- Requests/Sec

- Bytes Total/sec
- Transactions/Sec
- Errors During Script Runtime
- Request Wait Time
- Requests Executing
- Requests Not Found
- Requests Queued
- Requests Rejected
- Sessions Current

Advanced Settings for the ASP Server Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the ASP Server Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set one or more status thresholds criteria for each status condition per monitor instance. The status of the monitor and any associated alert action will be set based on comparison of all the threshold criteria you define for the monitor. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the ASP Server or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the ASP Server Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

15

BroadVision Application Server Monitor

The SiteScope BroadVision Application Server Monitor allows you to monitor the availability and performance statistics of a BroadVision server. The error and warning thresholds for the monitor can be set on one or more BroadVision server performance statistics.

This chapter describes:	On page:
About the BroadVision Application Server Monitor	159
Configuring the BroadVision Application Server Monitor	160

About the BroadVision Application Server Monitor

Use the BroadVision Application Server Monitor to monitor the server performance data for BroadVision servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate monitor instance for each BroadVision server in your environment.

You will need to know the Object Request Broker (ORB) port number for the BroadVision server you are trying to monitor.

In a BroadVision "Production" style environment where there is one primary root server and other secondary servers (for example, Interaction Manager node) on different machines, you can only define a monitor against the primary root node. Metrics for the other nodes in the configuration will be available for selection during root node monitor definition. In other words, monitoring is always accomplished through the primary root node, for all servers.

The default run schedule for this monitor is every 10 minutes, but you can change it to run more or less often using the **Frequency** setting.

Configuring the BroadVision Application Server Monitor

The BroadVision Application Server Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the BroadVision Application Server Monitor.

Main Settings for the BroadVision Application Server Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the BroadVision server, how often this BroadVision Application Server Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this BroadVision Application Server monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the BroadVision Application Server Monitor should system check the BroadVision server. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Server

Enter the BroadVision **root** server name of the BroadVision server you want to monitor. For example, 199.123.45.678.

Port

Enter the ORB port number to the BroadVision server you want to monitor. For example, 1221.

Counters

You use the features associated with the **Counters** setting to choose and manage the metrics you want to monitor with the BroadVision Application Server Monitor. Use the following steps to select and add counters.

To select or add counters:

1. Click **Get Counters** to query the remote system. After SiteScope has successfully connected to the remote system, the Get Counters selection dialogue opens.
2. Use the features in the Get Counters selection dialogue screen to select the BroadVision server metrics you want to monitor. Use the expandable menu controls as applicable to browse the available counters.
3. Use the check boxes to select between one and ten counters to be monitored.
4. Click **OK** to add the selected counters to the monitor configuration. The Get Counters selection dialogue closes and the monitor properties are updated with your selection.

Use the following steps to remove a counter from the selected counters list.

To remove or edit counters:

1. Click to edit the monitor for which you want to remove counters. Alternately, you may select the monitor you want to edit and click the Properties tab and click the **Edit** button. The monitor Properties screen opens.
2. Click the **Get Counters** button to open the Get Counters selection dialogue.
3. Clear the check box to the left of the current counter you want to remove.

   At this point, you may add other counters to the monitor by clicking the applicable check boxes.
4. Click **OK** at the bottom of the screen to update the monitor.

Advanced Settings for the BroadVision Application Server Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the BroadVision Application Server Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule

➤ Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

➤ Enable all associated alerts

➤ Disable all associated alerts for the next time period

➤ Disable all associated alerts on a one time schedule

➤ Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set one or more status thresholds criteria for each status condition per monitor instance. The status of the monitor and any associated alert action will be set based on comparison of all the threshold criteria you define for the monitor. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the BroadVision Application Server or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the BroadVision Application Server Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)

- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

16

Check Point Firewall-1 Monitor

The Check Point Firewall-1 Monitor allows you to monitor the statistics of a Check Point Firewall-1 using SNMP. The error and warning thresholds for the monitor can be set on one or more firewall statistics.

This chapter describes:	On page:
About the Check Point Firewall-1 Monitor	167
Configuring the Check Point Firewall-1 Monitor	167

About the Check Point Firewall-1 Monitor

Use the Check Point Firewall-1 Monitor to monitor the content of event logs and other data from Check Point Firewall-1 servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate Check Point Firewall-1 monitor instance for each Check Point Firewall-1 server in your environment.

The default run schedule for this monitor is every 10 minutes, but you can change it to run more or less often using the **Frequency** setting.

Configuring the Check Point Firewall-1 Monitor

The Check Point Firewall-1 Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the Check Point Firewall-1 Monitor.

Main Settings for the Check Point Firewall-1 Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the firewall, how often this Check Point Firewall-1 Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this Check Point Firewall-1 monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the Check Point Firewall-1 Monitor should system check the firewall. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Host Name

Enter the host name or IP address of the Check Point Firewall-1 server you want to monitor. The default is port 161. If the Check Point Firewall is configured to respond to SNMP on a different port number, enter the port number as part of the server address.

Counters

Choose the server performance parameters or counters you want to check with this monitor. The table list to the right of this item displays those currently selected for this monitor. Click **Get Counters** to bring up the counters selection screen. Check or clear the check boxes on the Get Counters screen to select one or more counters to monitor on this server. The performance parameters or counters available (with corresponding OID) for the Check Point Firewall-1 Monitor include:

- Rejected:1.3.6.1.4.1.2620.1.1.5
- Dropped:1.3.6.1.4.1.2620.1.1.6
- Logged:1.3.6.1.4.1.2620.1.1.7

- Major:1.3.6.1.4.1.2620.1.1.8
- Minor:1.3.6.1.4.1.2620.1.1.9
- Product:1.3.6.1.4.1.2620.1.1.10
- PointEvent:1.3.6.1.4.1.2620.1.1.11
- ModuleState:1.3.6.1.4.1.2620.1.1.1

Community

Enter the community name of the Check Point Firewall-1 you want to monitor. The **public** community is the default. You may need to consult with your network administrators about what community names are active in your network environment.

Advanced Settings for the Check Point Firewall-1 Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Check Point Firewall-1 Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Retry Delay

The number of seconds that the monitor should wait for a response from the server before retrying the request.

Timeout

The number of seconds that the monitor should wait for a response from the server before timing-out. Once this time period passes, the monitor will log an error and report an error status.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set one or more status thresholds criteria for each status condition per monitor instance. The status of the monitor and any associated alert action will be set based on comparison of all the threshold criteria you define for the monitor. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the Check Point Firewall-1 or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the Check Point Firewall-1 Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

17

Cisco Works Monitor

The Cisco Works Monitor allows you to monitor the statistics of a Cisco Works Server using SNMP. The error and warning thresholds for the monitor can be set on one or more Cisco Works server statistics.

This chapter describes:	On page:
About the Cisco Works Monitor	175
Configuring the Cisco Works Monitor	175

About the Cisco Works Monitor

Use the Cisco Works Monitor to monitor the content of event logs and other data from Cisco Works servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate Cisco Works monitor instance for each Cisco Works server in your environment.

The default run schedule for this monitor is every 10 minutes, but you can change it to run more or less often using the **Frequency** setting.

Configuring the Cisco Works Monitor

The Cisco Works Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the Cisco Works Monitor.

Main Settings for the Cisco Works Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the Cisco Works server, how often this Cisco Works Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this Cisco Works monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the Cisco Works Monitor should system check the Cisco Works server. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Server

Enter the name of the server you want to monitor.

SNMP Version

Select the version of SNMP to use when connecting.

Community

Enter the community name of the Cisco Works Server you want to monitor (valid only for version 1 or 2 connections). The **public** community is the default. You may need to consult with your network administrators about what community names are active in your network environment.

SNMP V3 Authentication Type

Select the type of authentication to use for version 3 connections.

SNMP V3 Username

Enter the username for version 3 connections.

SNMP V3 Authentication Password

Enter the authentication password to use for version 3 connections.

SNMP V3 Privacy Password

Enter the privacy password if DES privacy encryption is desired for version 3 connections. Leave blank if you do not want privacy.

SNMP V3 Context Engine ID

Enter a hexadecimal string representing the Context Engine ID to use for this connection. This is applicable for SNMP V3 only.

SNMP V3 Context Name

Enter the Context Name to use for this connection. This is applicable for SNMP V3 only.

Timeout

Enter the total time, in seconds, that SiteScope should wait for all SNMP requests (including retries) to complete.

Retries

Enter the number of times each SNMP GET request should be retried before SiteScope considers the request to have failed.

Port

Enter the port to use when requesting data from the SNMP agent. The default of 161 is the port on which an SNMP agent will typically be listening.

MIB File

Select either the Cisco Works MIB file or "All MIBs". Selecting the Cisco Works MIB file will cause only those objects that are described within that MIB file to be displayed. Selecting "All MIBs" will cause all objects discovered on the given Cisco Works server to be displayed when browsing counters. If no MIB information is available for an object, it is still displayed, but with no textual name or description.

Counters

You use the features associated with the **Counters** setting to choose and manage the metrics you want to monitor with the Cisco Works Monitor. Use the following steps to select and add counters.

To select or add counters:

1. Click **Get Counters** to query the remote system. After SiteScope has successfully connected to the remote system, the Get Counters selection dialogue opens.
2. Use the features in the Get Counters selection dialogue screen to select the Cisco Works server metrics you want to monitor. Use the expandable menu controls as applicable to browse the available counters.
3. Use the check boxes to select between one and ten counters to be monitored.
4. Click **OK** to add the selected counters to the monitor configuration. The Get Counters selection dialogue closes and the monitor properties are updated with your selection.

Use the following steps to remove a counter from the selected counters list.

To remove or edit counters:

1. Click to edit the monitor for which you want to remove counters. Alternately, you may select the monitor you want to edit and click the Properties tab and click the **Edit** button. The monitor Properties screen opens.
2. Click the **Get Counters** button to open the Get Counters selection dialogue.
3. Clear the check box to the left of the current counter you want to remove.

   At this point, you may add other counters to the monitor by clicking the applicable check boxes.
4. Click **OK** at the bottom of the screen to update the monitor.

The performance parameters or counters available (with corresponding OID) for the Cisco Works Monitor include:

- sysObjectID:1.3.6.1.2.1.1.2
- sysUpTime:1.3.6.1.2.1.1.3
- sysServices:1.3.6.1.2.1.1.7
- ifNumber:1.3.6.1.2.1.2.1
- ipForwarding:1.3.6.1.2.1.4.1
- ipDefaultTTL:1.3.6.1.2.1.4.2
- ipInReceives:1.3.6.1.2.1.4.3
- ipInHdrErrors:1.3.6.1.2.1.4.4
- ipInAddrErrors:1.3.6.1.2.1.4.5
- ipForwDatagrams:1.3.6.1.2.1.4.6
- ipInUnknownProtos:1.3.6.1.2.1.4.7
- ipInDiscards:1.3.6.1.2.1.4.8
- ipInDelivers:1.3.6.1.2.1.4.9
- ipOutRequests:1.3.6.1.2.1.4.10
- ipOutDiscards:1.3.6.1.2.1.4.11
- ipOutNoRoutes:1.3.6.1.2.1.4.12
- ipReasmTimeout:1.3.6.1.2.1.4.13
- ipReasmReqds:1.3.6.1.2.1.4.14
- ipReasmOKs:1.3.6.1.2.1.4.15
- ipReasmFails:1.3.6.1.2.1.4.16
- ipFragOKs:1.3.6.1.2.1.4.17
- ipFragFails:1.3.6.1.2.1.4.18
- ipFragCreates:1.3.6.1.2.1.4.19
- icmpOutAddrMaskReps:1.3.6.1.2.1.5.26
- tcpRtoAlgorithm:1.3.6.1.2.1.6.1
- tcpRtoMin:1.3.6.1.2.1.6.2
- tcpRtoMax:1.3.6.1.2.1.6.3
- tcpMaxConn:1.3.6.1.2.1.6.4
- tcpActiveOpens:1.3.6.1.2.1.6.5
- tcpPassiveOpens:1.3.6.1.2.1.6.6
- tcpAttemptFails:1.3.6.1.2.1.6.7
- tcpEstabResets:1.3.6.1.2.1.6.8
- tcpCurrEstab:1.3.6.1.2.1.6.9
- tcpInSegs:1.3.6.1.2.1.6.10
- tcpOutSegs:1.3.6.1.2.1.6.11
- tcpRetransSegs:1.3.6.1.2.1.6.12
- tcpInErrs:1.3.6.1.2.1.6.14
- tcpOutRsts:1.3.6.1.2.1.6.15
- udpInDatagrams:1.3.6.1.2.1.7.1
- udpNoPorts:1.3.6.1.2.1.7.2
- udplInErrors:1.3.6.1.2.1.7.3
- udpOutDatagrams:1.3.6.1.2.1.7.4
- snmpInPkts:1.3.6.1.2.1.11.1
- snmpOutPkts:1.3.6.1.2.1.11.2
- snmpInBadVersions:1.3.6.1.2.1.11.3
- snmpInBadCommunityNames:1.3.6.1.2.1.11.4

- ipRoutingDiscards:1.3.6.1.2.1.4.23
- icmpInMsgs:1.3.6.1.2.1.5.1
- icmpInErrors:1.3.6.1.2.1.5.2
- icmpInDestUnreachs:1.3.6.1.2.1.5.3
- icmpInTimeExcds:1.3.6.1.2.1.5.4
- icmpInParmProbs:1.3.6.1.2.1.5.5
- icmpInSrcQuenchs:1.3.6.1.2.1.5.6
- icmpInRedirects:1.3.6.1.2.1.5.7
- icmpInEchos:1.3.6.1.2.1.5.8
- icmpInEchosReps:1.3.6.1.2.1.5.9
- icmpInTimestamps:1.3.6.1.2.1.5.10
- icmpInTimestampsReps:1.3.6.1.2.1.5.11
- icmdplnAddrMasks:1.3.6.1.2.1.5.12
- icmpInAddrMaskReps:1.3.6.1.2.1.5.13
- icmpOutMsgs:1.3.6.1.2.1.5.14
- icmpOutErrors:1.3.6.1.2.1.5.15
- icmpOutDestUnreachs:1.3.6.1.2.1.5.16
- icmpOutIimeExcds:1.3.6.1.2.1.5.17
- icmpOutParmProbs:1.3.6.1.2.1.5.18
- icmpOutSrcQuenchs:1.3.6.1.2.1.5.19
- icmpOutRedirects:1.3.6.1.2.1.5.20
- snmpInBadCommunityUses:1.3.6.1.2.1.11.5
- snmpInASNParseErrs:1.3.6.1.2.1.11.6
- snmpInTooBigs:1.3.6.1.2.1.11.8
- snmpInNoSuchNames:1.3.6.1.2.1.11.9
- snmpInBadValues:1.3.6.1.2.1.11.10
- snmpInReadOnlys:1.3.6.1.2.1.11.11
- snmpInGenErrs:1.3.6.1.2.1.11.12
- snmpInTotalReqVars:1.3.6.1.2.1.11.13
- snmpInTotalSetVars:1.3.6.1.2.1.11.14
- snmpInGetRequests:1.3.6.1.2.1.11.15
- snmpInGetNexts:1.3.6.1.2.1.11.16
- snmpInSetRequests:1.3.6.1.2.1.17.1
- snmpInGetResponses:1.3.6.1.2.1.18.1
- snmpInTraps:1.3.6.1.2.1.11.19
- snmpOutTooBigs:1.3.6.1.2.1.11.20
- snmpOutNoSuchNames:1.3.6.1.2.1.11.21
- snmpOutBadValues:1.3.6.1.2.1.11.22
- snmpOutGenErrs:1.3.6.1.2.1.11.24
- snmpOutGetRequests:1.3.6.1.2.1.11.25
- snmpOutGetNexts:1.3.6.1.2.1.11.26
- snmpOutSetRequests:1.3.6.1.2.1.11.27

- icmpOutEchos:1.3.6.1.2.1.5.21
- icmpOutEchoReps:1.3.6.1.2.1.5.22
- icmpOutTimestamps:1.3.6.1.2.1.5.23
- icmpOutTimestampReps:1.3.6.1.2.1.5.24
- icmpOutAddrMasks:1.3.6.1.2.1.5.25
- snmpOutGetResponses:1.3.6.1.2.1.11.28
- snmpOutTraps:1.3.6.1.2.1.11.1
- snmpEnableAuthenTraps:1.3.6.1.2.1.11.1

Advanced Settings for the Cisco Works Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Cisco Works Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Counter Calculation Mode

Use this option to perform a calculation on objects of type Counter, Counter32, or Counter64. The available calculations are:

➤ a simple delta of the current value from the previous value, OR

➤ a rate calculation using the delta of current value from previous value, divided by the time elapsed between measurements

---

Note: This option only applies to the aforementioned object types. A Cisco Works Monitor that monitors Counter objects as well as DisplayString objects will only perform this calculation on the Counter objects.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule

➤ Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set one or more status thresholds criteria for each status condition per monitor instance. The status of the monitor and any associated alert action will be set based on comparison of all the threshold criteria you define for the monitor. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the Cisco Works or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the Cisco Works Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

18

Citrix Server Monitor

The SiteScope Citrix Server Monitor allows you to monitor the availability of an Citrix MetaFrame servers (MetaFrame 1.8 Service Pack 3, MetaFrame XP(s,a,e) Feature Release 1/Service Pack 1, and MetaFrame XP(s,a,e) Feature Release 2/Service Pack 2). The error and warning thresholds for the monitor can be set on one or more Citrix Server performance statistics.

This chapter describes:	On page:
About the Citrix Server Monitor	187
Configuring the Citrix Server Monitor	188
Troubleshooting Tips for the Citrix Server Monitor	195

About the Citrix Server Monitor

The Citrix Server Monitor makes use of Performance Counters to measure application server performance. SiteScope will need to be running under an account that has the necessary administrative security privileges to access performance counter data from remote servers. If the servers you want to monitor are in a different domain, are governed under a different policy, or require a unique login different than the account SiteScope is running under, then you will need to define the connection to these servers under the NT Remotes option in the SiteScope Preferences.

The Citrix Server Monitor allows you to monitor the server performance statistics from Citrix Metaframe Servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate Citrix monitor instance for each Citrix Server in your environment.

The following are important requirements for using the SiteScope Citrix Server Monitor:

- The Remote Registry service must be running on the machine where the Citrix Server is running if Citrix is running on a Windows 2000 platform.
- The Citrix Resource Manager must available, installed, and running on the Citrix servers you want to monitor.
- One or more Citrix vusers need to have established a connection with the Citrix server in order to enable viewing of ICA Session object.

Configuring the Citrix Server Monitor

The Citrix Server Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the Citrix Server Monitor.

Main Settings for the Citrix Server Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the Citrix server, how often this Citrix Server Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this Citrix Server monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the Citrix Server Monitor should check or test the Citrix server. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Server

Choose the server where the Citrix Server you want to monitor is running. Use the drop-down list to select a server from the list of remote servers that are available to the SiteScope agent.

Counters

You use the features associated with the **Counters** setting to choose and manage the metrics you want to monitor with the Citrix Server Monitor. Use the following steps to select and add counters.

To select or add counters:

1. Click **Get Counters** to query the remote system. After SiteScope has successfully connected to the remote system, the Get Counters selection dialogue opens.
2. Use the features in the Get Counters selection dialogue screen to select the Citrix server metrics you want to monitor. Use the expandable menu controls as applicable to browse the available counters.
3. Use the check boxes to select between one and ten counters to be monitored.
4. Click **OK** to add the selected counters to the monitor configuration. The Get Counters selection dialogue closes and the monitor properties are updated with your selection.

Use the following steps to remove a counter from the selected counters list.

To remove or edit counters:

1. Click to edit the monitor for which you want to remove counters. Alternately, you may select the monitor you want to edit and click the Properties tab and click the **Edit** button. The monitor Properties screen opens.

2 Click the **Get Counters** button to open the Get Counters selection dialogue.

3 Clear the check box to the left of the current counter you want to remove.

At this point, you may add other counters to the monitor by clicking the applicable check boxes.

4 Click **OK** at the bottom of the screen to update the monitor.

Note: You will not see the counters listed for the ICA Session object until the Citrix vusers have established a connection with the Citrix server. You will have to initialize or run the Citrix vuser first and then configure the SiteScope Citrix Monitor to add the counters for the ICA Session object.

The performance parameters or counters available for the Citrix Server Monitor include:

- Latency - Last Recorded
- Latency - Session Average
- Latency - Session Deviation
- Output Session Bandwidth
- Input Session Bandwidth
- Output Session Compression
- Input Session Compression
- Output LPT 1 Bandwidth
- Input LPT 1 Bandwidth
- Output LPT 2 Bandwidth
- Input LPT 2 Bandwidth
- Output COM 1 Bandwidth
- Input COM 1 Bandwidth
- Output COM 2 Bandwidth
- Input COM 2 Bandwidth
- Output Printer Bandwidth
- Input Printer Bandwidth
- Output COM Bandwidth
- Input COM Bandwidth
- Output Drive Bandwidth
- Input Drive Bandwidth
- Output Clipboard Bandwidth
- Input Clipboard Bandwidth
- Output ThinWire Bandwidth

- Input ThinWire Bandwidth
- Output Audio Bandwidth
- Input Audio Bandwidth
- Output Management Bandwidth
- Input Management Bandwidth
- Output Licensing Bandwidth
- Input Licensing Bandwidth
- Output VideoFrame Bandwidth
- Input VideoFrame Bandwidth
- Output PN Bandwidth
- Input PN Bandwidth
- Output Seamless Bandwidth
- Input Seamless Bandwidth
- Output Font Data Bandwidth
- Input Font Data Bandwidth
- Output Text Echo Bandwidth
- Input Text Echo Bandwidth
- Output Control Channel Bandwidth
- Input Control Channel Bandwidth

Advanced Settings for the Citrix Server Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Citrix Server Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set one or more status thresholds criteria for each status condition per monitor instance. The status of the monitor and any associated alert action will be set based on comparison of all the threshold criteria you define for the monitor. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the Citrix Server or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the Citrix Server Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

Troubleshooting Tips for the Citrix Server Monitor

The following are troubleshooting tips for the Citrix Server Monitor.

1. Open a command line window (DOS prompt)
2. Type the following command, substituting the hostname as appropriate:

   ```
   C:\>perfex \\hostname -u username -p password -h | find "ICA"
   ```

3. This should return a response like the following:

   ```
   (3378) ICA Session
   (3386) ICA Session
   (3379) This object has several counters that can be used to monitor the
   performance in ICA sessions
   (3387) This object has several counters that can be used to monitor the
   performance in ICA sessions"
   ICA Session" 3386    performance in ICA sessions
   ```

   If you do not see something like the above response, then either the counters are not available on the remote server or you will get a more descriptive error message indicating what might be the problem.

19

Composite Monitor

The Composite Monitor is designed to simplify the monitoring of complex network environments by checking the status readings of a set of other SiteScope monitors and/or monitor groups.

This chapter describes:	On page:
About the Composite Monitor	197
Configuring the Composite Monitor	198

About the Composite Monitor

Each time the Composite Monitor runs, it returns a status based on the number and percentage of items in the specified monitors and/or groups currently reporting an error, warning, or OK status. It writes the percentages reported in the monitoring log file.

One reason you should use this monitor is if you want to create complex monitor alert logic. For example, if you wanted to trigger an alert when:

- 5 or more monitors in a group of 8 are in error
- 3 or more groups have monitors with errors in them
- of two monitors, exactly 1 in error

then you could create a Composite Monitor that went into error on these conditions, and then add alerts on the Composite Monitor to take the desired actions.

If you need alert logic that is more complex than SiteScope's standard alerts will allow, you may be able to use the Composite Monitor to create a customized alert behavior.

About Scheduling This Monitor

The Composite Monitor is very lightweight, so schedule it to run at least as often as the most frequent monitor that it is watching.

Configuring the Composite Monitor

The Composite Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the Composite Monitor.

Main Settings for the Composite Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the systems, how often this Composite Monitor instance should be run, and the text name used for this monitor instance. See “Common Monitor Settings” in the chapter “Working with SiteScope Monitors” for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this Composite monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the Composite Monitor should system check the systems. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Items

Choose one or more (using control-click) monitors and/or groups that the Composite Monitor will be comprised of.

Advanced Settings for the Composite Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Composite Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Run Monitors

Check this box if you want the Composite Monitor to control the scheduling of the selected monitors, as opposed to just checking their status readings. Any monitors that are to be run this way should not also be run separately, so edit the individual monitors, blank out the **Update Every** box for that monitor, and save the changes. Those monitors will then only run when scheduled by the Composite Monitor. This is useful if you want the monitors to run one after another or run at approximately the same time.

Monitor Delay

If Run Monitors is checked, this is the number of seconds to wait between running each monitor. This setting is useful if you need to wait for processing to occur on your systems before running the next monitor.

Check All Monitors in Group(s)

By default, a group is checked and counted as a single item when checking status readings. If this box is checked, all of the monitors in selected groups (and their subgroups) are checked and counted.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set up to ten status thresholds criteria for each status condition per monitor instance. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the Composite or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the Composite Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

20

ColdFusion Server Monitor

The ColdFusion Server Monitor allows you to monitor the availability of an Allaire ColdFusion server (versions 4.5x) on Windows NT systems. The error and warning thresholds for the monitor can be set on one or more ColdFusion server performance statistics.

This chapter describes:	On page:
About the ColdFusion Server Monitor	205
Configuring the ColdFusion Server Monitor	206

About the ColdFusion Server Monitor

The ColdFusion Server Monitor makes use of Performance Counters to measure application server performance. SiteScope will need to be running under an account that has the necessary administrative security privileges to access performance counter data from remote servers. If the servers you want to monitor are in a different domain, are governed under a different policy, or require a unique login different than the account SiteScope is running under, then you will need to define the connection to these servers under the NT Remote Preferences option in the SiteScope Preferences container.

Use the ColdFusion Monitor to monitor the server performance statistics from ColdFusion servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate ColdFusion monitor instance for each ColdFusion server in your environment.

The Remote Registry service must be running on the machine where the ColdFusion server is running if ColdFusion is running on Windows 2000.

The default run schedule for this monitor is every 10 minutes, but you can change it to run more or less often using the **Frequency** setting.

Configuring the ColdFusion Server Monitor

The ColdFusion Server Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the ColdFusion Server Monitor.

Main Settings for the ColdFusion Server Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the ColdFusion server, how often this ColdFusion Server Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this ColdFusion Server monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the ColdFusion Server Monitor should system check the ColdFusion server. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Server

Choose the server where the ColdFusion Server you want to monitor is running. Use the drop-down list to select a server from the list of remote servers that are available to the SiteScope agent.

Counters

You use the features associated with the **Counters** setting to choose and manage the metrics you want to monitor with the ColdFusion Server Monitor. Use the following steps to select and add counters.

To select or add counters:

1. Click **Get Counters** to query the remote system. After SiteScope has successfully connected to the remote system, the Get Counters selection dialogue opens.
2. Use the features in the Get Counters selection dialogue screen to select the ColdFusion server metrics you want to monitor. Use the expandable menu controls as applicable to browse the available counters.
3. Use the check boxes to select between one and ten counters to be monitored.
4. Click **OK** to add the selected counters to the monitor configuration. The Get Counters selection dialogue closes and the monitor properties are updated with your selection.

Use the following steps to remove a counter from the selected counters list.

To remove or edit counters:

1. Click to edit the monitor for which you want to remove counters. Alternately, you may select the monitor you want to edit and click the Properties tab and click the **Edit** button. The monitor Properties screen opens.
2. Click the **Get Counters** button to open the Get Counters selection dialogue.
3. Clear the check box to the left of the current counter you want to remove.

   At this point, you may add other counters to the monitor by clicking the applicable check boxes.
4. Click **OK** at the bottom of the screen to update the monitor.

The performance parameters or counters available for the ColdFusion Server Monitor include:

- Avg DB Time (msec)
- Avg Queue Time (msec)

- Avg Req Time (msec)
- Bytes In/Sec
- Bytes Out/Sec
- Cache Pops/Sec
- DB Hits/Sec
- Page Hits/Sec
- Queued Requests
- Running Requests

Advanced Settings for the ColdFusion Server Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the ColdFusion Server Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set one or more status thresholds criteria for each status condition per monitor instance. The status of the monitor and any associated alert action will be set based on comparison of all the threshold criteria you define for the monitor. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the ColdFusion Server or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the ColdFusion Server Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

21

CPU Utilization Monitor

The CPU Utilization Monitor reports the percentage of CPU time that is currently being used on the server. It is important to watch CPU usage on your Web server to see that it does not become overloaded on a regular basis.

This chapter describes:	On page:
About the CPU Utilization Monitor	213
Configuring the CPU Utilization Monitor	214

About the CPU Utilization Monitor

When CPU usage becomes too high, clients and customers will either find the system response time has become very slow, or if applications hang as a result of high CPU usage, they simply will not be able to access it. Therefore, it is very important to monitor CPU usage and do something about high usage before it results in outages or poor response times.

Whether the servers in your infrastructure are running with a single CPU or with multiple CPUs, you only need to create one CPU monitor per remote server. If you have multiple CPUs, SiteScope will report on the average usage for all of them.

About Scheduling this Monitor

In general, the CPU Monitor does not need to be run as often as some of the other monitors. If you do not usually suffer from CPU problems, you can run it less frequently - perhaps every half hour or so. If you are prone to CPU usage problems, you should run it more frequently. All machines will have short spikes of CPU usage, but the primary thing that you are looking for is high usage on a regular basis. This indicates that your system is overloaded and that you need to look for a cause.

Status

The Status reading is the current value returned by this monitor; for example, 68% used. SiteScope displays an average for multiple CPU systems. On NT, this is the average CPU usage between runs of the monitor. On UNIX, this is the instantaneous CPU when the monitor runs.

The status is logged as either OK or warning. A warning status is returned if the CPU is in use more than 90% of the time.

Configuring the CPU Utilization Monitor

The CPU Utilization Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the CPU Utilization Monitor.

Main Settings for the CPU Utilization Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the remote server CPU, how often this CPU Utilization Monitor instance should be run, and the text name used for this monitor instance. See “Common Monitor Settings” in the chapter “Working with SiteScope Monitors” for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this CPU Utilization monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the CPU Utilization Monitor should CPU usage check the remote server CPU. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Server

Choose the server for which you want to monitor CPU Utilization. Use the drop-down list to select a server from the list of remote servers that are available to the SiteScope agent.

Advanced Settings for the CPU Utilization Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the CPU Utilization Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set up to ten status thresholds criteria for each status condition per monitor instance. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the CPU Utilization or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the CPU Utilization Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

22

Database Counter Monitor

The SiteScope Database Counter Monitor allows you to monitor the availability of any database through a JDBC driver. The error and warning thresholds for the monitor can be set on one or more database server performance statistics.

This chapter describes:	On page:
About the Database Counter Monitor	221
Editing the Database Counter Monitor	223

About the Database Counter Monitor

Use the Database Counter Monitor to make SQL queries for performance metrics from any JDBC-accessible database. This monitor provides optional support for calculating deltas and rates for metrics between monitor runs. You can monitor multiple counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning.

The following are several key requirements for using the Database Counter Monitor:

- You must have a copy of the applicable JDBC database driver file (for example, the Oracle thin driver is packaged in a file called classes12.zip) on the SiteScope server. Copy the downloaded driver file into the <SiteScope install path>\SiteScope\java\lib\ext subdirectory. If the file is in zip format, DO NOT unzip the file. Stop and restart the SiteScope service after copying the driver file to the SiteScope machine.

- You must supply the correct **Database Connection URL**, a database username and password when setting up the monitor. The syntax of the Database Connection URL may vary depending on which JDBC driver and which type of database you wish to monitor. For example to monitor an Oracle database using the Oracle thin driver, the URL you need to use has the form:

  jdbc:oracle:thin:@<host>:<tcp port>:<database sid>

  To monitor a Postgresql database, the URL is of the form:

  jdbc:postgresql://<host>:<port>/<database>

- You must specify the Database Driver that was installed on the SiteScope server when setting up the monitor. The Database Driver is just the name of a Java class in X.Y.Z format. For example, the Database Driver for the Oracle thin JDBC driver is:

  oracle.jdbc.driver.OracleDriver

  and the Database Driver for the Postgresql JDBC driver is:

  org.postgresql.Driver

- Generally, you should only have one instance of each type of JDBC driver client installed on the SiteScope machine. If there is more than one instance installed, SiteScope may report an error and be unable to connect to the database. For example, installing two classes12.zip files from two different versions of Oracle will probably not work.

- You must have a database user login that SiteScope will use to access the database. SiteScope will only be able to execute the SQL queries that this user has permission to execute on the database.

The default run schedule for this monitor is every 10 minutes, but you can change it to run more or less often using the Update every setting.

Editing the Database Counter Monitor

The Database Counter Monitor is part of the Oracle Solution. This monitor type can only be added by deploying an Oracle Solution template. Once the monitor has been created, you can edit the configuration of the monitor the same as other monitors. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the Database Counter Monitor.

Main Settings for the Database Counter Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the database, how often this Database Counter Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this Database Counter monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the Database Counter Monitor should database query the database. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Server

Select the server you want to monitor. Use the drop-down menu to view a list of servers or to enter the connection URL to the database.

Database Connection URL

Enter the connection URL to the database you want to monitor. For example, jdbc:oracle:thin:@192.168.0.50:1521:ORCL.

Query

Enter an SQL query that returns at least two columns of data. The values in the first column of data are interpreted as the labels for the entries in the each row. The values in the first row are treated as labels for each entry in the column.

Database User Name

Enter the user name that SiteScope should use to connect to the database.

Database Password

Enter the password for the user name that SiteScope should use to connect to the database.

Database Driver

Enter the driver used to connect to the database. For example, org.postgresql.Driver.

Connection Timeout

Enter an optional time out value, in seconds, that SiteScope should wait for a database connection to respond. If the database connection can not be completed within the period specified, SiteScope will report an error.

Note: The sum of the Connection Timeout value and Query Timeout value should always be less than the Update every value for the monitor. For example, if the monitor Update every value is set to 10 minutes, this equates to 600 seconds.

Query Timeout

Enter an optional time out value, in seconds, that SiteScope should wait for a response from the database query. If the database does not respond within the period specified, SiteScope will report an error.

Note: The sum of the Connection Timeout value and Query Timeout value should always be less than the Update every value for the monitor. For example, if the monitor Update every value is set to 10 minutes, this is equivalent to 600 seconds. If both the Connection Timeout value and Query Timeout value are set to 120 seconds, the sum of these would be 240 seconds.

Note: Some commonly used databases and database drivers do not support the query timeout feature. In these cases the Query Timeout value should be set to zero.

Counters

You use the features associated with the **Counters** setting to choose and manage the metrics you want to monitor with the Database Counter Monitor. Use the following steps to select and add counters.

To select or add counters:

1. Click **Get Counters** to query the remote system. After SiteScope has successfully connected to the remote system, the Get Counters selection dialogue opens.
2. Use the features in the Get Counters selection dialogue screen to select the database metrics you want to monitor. Use the expandable menu controls as applicable to browse the available counters.
3. Use the check boxes to select between one and ten counters to be monitored.
4. Click **OK** to add the selected counters to the monitor configuration. The Get Counters selection dialogue closes and the monitor properties are updated with your selection.

Use the following steps to remove a counter from the selected counters list.

To remove or edit counters:

1. Click to edit the monitor for which you want to remove counters. Alternately, you may select the monitor you want to edit and click the Properties tab and click the **Edit** button. The monitor Properties screen opens.
2. Click the **Get Counters** button to open the Get Counters selection dialogue.
3. Clear the check box to the left of the current counter you want to remove.

   At this point, you may add other counters to the monitor by clicking the applicable check boxes.
4. Click **OK** at the bottom of the screen to update the monitor.

Advanced Settings for the Database Counter Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Database Counter Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Divisor Query

An SQL query which will return a single numeric value. The value of each counter is calculated by dividing the counter value as retrieved from the database divided by the Divisor Query value.

DB Machine Name

The identifier for the target database server, as it should be reported to Mercury Business Availability Center.

No Cumulative Counters

Selecting this checkbox turns off the default behavior of calculating the value of a counter as the difference between that counter's cumulative values (as retrieved from the database on consecutive monitor runs).

No Divide Counters

Selecting this checkbox turns off the default behavior of calculating the value of a counter as the value retrieved from the database (or the delta of two values retrieved from the database over consecutive monitor runs) divided by some number. The divisor is either taken from the Divisor Query, or it is the elapsed time in seconds since the previous monitor run.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set one or more status thresholds criteria for each status condition per monitor instance. The status of the monitor and any associated alert action will be set based on comparison of all the threshold criteria you define for the monitor. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the Database Counter or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1 Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.

2 Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.

3 Enter a value applicable to the measurement parameter in the third text box.

4 To add another threshold setting, click the **New Error If** button and repeat the steps above.

5 Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the Database Counter Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see “Common Monitor Settings” in the chapter Chapter 2, “Working with SiteScope Monitors.”

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see “Working with Categories” in *Working with Monitor Administration*.

23

Database Query Monitor

The Database Query Monitor checks that a database is working correctly by connecting to it and performing a query. Optionally, it can check the results of a database query for expected content.

This chapter describes:	On page:
About the Database Query Monitor	233
Setup Requirements for the Database Query Monitor	234
Configuring the Database Query Monitor	235
Technical Notes on Monitoring Common Databases	243

About the Database Query Monitor

If your database application is not working properly, the user may not be able to access Web content and forms that depend on the database. Most importantly, the user will not be able to complete e-commerce transactions that are supported by databases. The other reason to monitor database queries is so you can find performance bottlenecks. If the database interaction time and the associated user URL retrieval times are both increasing at about the same amount, the database is probably the bottleneck. If not, the bottleneck is probably somewhere else in the network.

Usually the most important thing to monitor in databases are the queries used by your most frequently used and most important Web applications. If more than one database is used, you will want to monitor each of the databases.

Each time the Database Query Monitor runs, it returns a status, the time it takes to perform the query, the number of rows in the query result, and the first two fields in the first row of the result and writes them in the monitoring log file.

You may also choose to monitor internal database statistics. The statistics provided by each database are different but may include items such as database free space, transaction log free space, transactions/second, and average transaction duration.

You may want to monitor your most critical and most common queries frequently, every 2-5 minutes. Database statistics that change less frequently can be monitored every 30 or 60 minutes.

Setup Requirements for the Database Query Monitor

The steps for setting up a Database Query Monitor will vary according to what database software you are trying to monitor. The following is an overview of the requirements for using the Database Query Monitor:

- You must install or copy a compatible database driver or database access API into the appropriate SiteScope directory location. Many database driver packages are available as compressed (zipped) archive files or .jar files. Database drivers in this form must NOT be extracted and must be installed into the **<SiteScope install path>/SiteScope/java/lib/ext** subdirectory.
- You need to know the syntax for accessing the database driver. Examples of database driver path strings are:
  - sun.jdbc.odbc.JdbcOdbcDriver - (JDBC-ODBC Bridge Driver from Sun Microsystems)
  - com.inet.tds.TdsDriver - (TDS driver from i-net Software for Microsoft SQL databases)
  - oracle.jdbc.driver.OracleDriver - (JDBC thin driver for Oracle 7 and 8 databases)
- You need to know the syntax for the Database Connection URL. The Database Connection URL normally includes the class of driver you are

using, some key name relating to the supplier of the driver software, followed by a combination of server, host, and port identifiers. Examples of database connection URLs are:

- jdbc:odbc:*dsname* - (where *dsname* is the data source name in the system environment or configuration)
- jdbc:inetdae:*hostname*:*port* - (where *hostname* is the name of the host where the database is running and *port* is the port on which the database interfaces with the driver)
- jdbc:oracle:thin:@*hostname*:*port*:*dbname* - (where *hostname* is the name of the host where the database is running, *port* is the port on which the database interfaces with the driver, and *dbname* is the name of the Oracle database instance)

➤ The database you want to monitor needs to be running, have a database name defined, and have at least one named table created in the database. In some cases, the database management software needs to be configured to allow connections via the middleware or database driver.

➤ You need a valid username and password to access and perform a query on the database. In some cases, the machine and user account that SiteScope is running on must be given permissions to access the database.

➤ You need to know a valid SQL query string for the database instance and database table(s) in the database you want to monitor. Consult your database administrator to work out appropriate queries to test.

Configuring the Database Query Monitor

The Database Query Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the Database Query Monitor.

Main Settings for the Database Query Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the remote database, how often this Database Query Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this Database Query monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the Database Query Monitor should database query the remote database. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Database Connection URL

Enter a URL to a Database Connection. One way to create a database connection is to use ODBC to create a named connection to a database. For example, first use the ODBC control panel to create a connection called test. Then, enter jdbc:odbc:test in this box as the connection URL.

Query

Enter the SQL query to test. For example, select * from sysobjects.

Database Driver

Enter the java class name of the JDBC database driver. The default, sun.jdbc.odbc.JdbcOdbcDriver, uses ODBC to make Database connections. SiteScope uses the same database driver for both primary and backup database connections. If a custom driver is used, the driver must also be installed in the **SiteScope/java** directory.

Advanced Settings for the Database Query Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Database Query Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Match Content

Enter a string of text to check for in the query result. If the text is not contained in the result, the monitor will display no match on content. The search is case sensitive. This works for XML tags as well.

You may also perform a Perl regular expression match by enclosing the string in forward slashes, with an "i" after the trailing slash indicating case-insensitive matching. (For example, /href=Doc\d+\.html/ or /href=doc\d+\.html/i). If you want a particular piece of text to be saved and displayed as part of the status, use parentheses in a Perl regular expression. For example /Temperature: (\d+)/. This would return the temperature as it appears on the page and this could be used when setting an Error if or Warning if threshold.

Database Username

Enter the username used to login to the database. If you are using Microsoft SQL server and the default driver (Sun Microsystem JDBC ODBC bridge driver (sun.jdbc.odbc.JdbcOdbcDriver), you can leave this blank and choose NT Authentication when you setup the ODBC connection. With NT Authentication, SiteScope will connect using the login account of the SiteScope service.

Database Password

Enter a password used to login to the database. If you are using Microsoft SQL server and the default driver (Sun Microsystem JDBC ODBC bridge driver (sun.jdbc.odbc.JdbcOdbcDriver), you can leave this blank and choose NT Authentication when you create the ODBC connection. With NT Authentication, SiteScope will connect using the login account of the SiteScope service.

File Path

The Database Query Monitor can read a database query from a file. Enter the name of the file that contains the query you want to run. The file should be a simple text format. Use this feature as an alternative to the Query box above for complex queries or queries that change and are updated by an external application.

Connection Timeout

Enter a timeout value, in seconds, that the monitor should wait for a database connection.

Note: The sum of the Connection Timeout value and Query Timeout value should always be less than the **Frequency** value for the monitor.

Query Timeout

Enter a timeout value, in seconds, that the monitor should wait for a database query to return results.

Note: The sum of the Connection Timeout value and Query Timeout value should always be less than the **Frequency** value for the monitor.

Some commonly used databases and database drivers do not support the query timeout feature. In these cases the Query Timeout value should be set to zero.

Column Labels

Enter the field labels for the two columns returned by the query, separated by a ",". The field labels should be two of the labels that are returned by the Query string entered above. These column labels are used as data labels in SiteScope reports for Database Query Monitors.

DB Machine Name

If you are reporting monitor data to an installation of Mercury Business Availability Center, enter a text identifier describing the database server that this monitor is monitoring. This text descriptor is used to identify the database server when the monitor data is viewed in a Mercury Business Availability Center report. Use only alphanumeric characters for this entry. You can enter the name of the monitored server or a description of the database.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set up to ten status thresholds criteria for each status condition per monitor instance. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the Database Query or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.

3 Enter a value applicable to the measurement parameter in the third text box.

4 To add another threshold setting, click the **New Error If** button and repeat the steps above.

5 Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the Database Query Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

Technical Notes on Monitoring Common Databases

This section provides some technical notes and requirements for using the Database QueryMonitor to monitor several common databases.

Accessing Oracle Databases Without Using ODBC

If you want to monitor an Oracle database without using ODBC, a good alternative is to use the Oracle Thin JDBC Drivers.

To set up SiteScope to use the JDBC Thin Drivers:

1. Download the Oracle Thin JDBC drivers from http://technet.oracle.com/software/download.htm (may require service/support agreement with Oracle)
2. Copy the downloaded driver package into the **<SiteScope install path>/SiteScope/java/lib/ext** subdirectory.

Note: Do not extract the files from the archive file.

---

3. Stop and restart the SiteScope service.
4. Now, use your browser to add a Database Query Monitor within SiteScope.

   The **Database Connection URL** format for the Oracle JDBC driver is:

   jdbc:oracle:thin:@<tcp address>:<tcp port>:<database SID>

   For example to connect to the ORCL database on a machine using port 1521 you would use:

   jdbc:oracle:thin:@206.168.191.19:1521:ORCL

Note: After the word "thin" is a colon (:) and then the "@" symbol

---

The **Database Driver** for the Oracle thin JDBC driver is:

oracle.jdbc.driver.OracleDriver

Enter this string into the **Database Driver** text box under the Advanced Settings section of the Add Database Query Monitor form.

Possible Errors Using the Oracle Thin Driver

- "*error, connect error, No suitable driver*": check for syntax errors in "Database Connection URL", such as dots instead of colons
- "*error, connect error, Io exception: The Network Adapter could not establish the connection*": in "Database Connection URL", check jdbc:oracle:thin:@206.168.191.19:1521:ORCL
- "*error, connect error, Io exception: Invalid connection string format, a valid format is: "host:port:sid*": in "Database Connection URL", check jdbc:oracle:thin:@206.168.191.19:1521:ORCL
- "*error, connect error, Invalid Oracle URL specified: OracleDriver.connect*": in "Database Connection URL", check for a colon before the "@" jdbc:oracle:thin@206.168.191.19:1521:ORCL
- "*Refused:OR=(CODE=12505)(EMFI=4))))*": in "Database Connection URL", check the database SID is probably incorrect (ORCL part). This error can also occur when the tcp address, or tcp port is incorrect. If this is the case, verify the tcp port and check with the your database administrator to verify the proper SID.
- "*String Index out of range: -1*": in "Database Connection URL", check for the database server address, port, and the database SID.
- "*error, driver connect error, oracle.jdbc.driver.OracleDriver*": check syntax in item "Database Driver"
- "*error, driver connect error, oracle.jdbc.driver.OracleDriver*": check that driver is loaded in correct place

- "*error, connect error, No suitable driver*": check driver specified in item "Database Driver"
- "*error, connect error, No suitable driver*": check for syntax errors in "Database Connection URL", such as dots instead of colons

Monitoring Informix Databases

Monitoring a Informix database requires the use of a JDBC driver.

To enable SiteScope to monitor an Informix database:

1. Download the Informix JDBC driver from Informix. See the Informix Web site for details.
2. Uncompress the distribution file
3. Open a DOS window and go to the jdbc140jc2 directory
4. Unpack the driver by running the following command:

   c:\SiteScope\java\bin\java -cp . setup

5. Copy ifxjdbc.jar to the <**SiteScope install path**>**SiteScope****java****ext****bin**\ subdirectory.
6. Stop and restart SiteScope
7. Now, use your browser to add a Database Query Monitor within SiteScope.

   The **Database Connection URL** format for the Informix JDBC driver is:

   jdbc:informix-sqli://<database hostname>:<tcp port><database server>:INFORMIXSERVER=<database>

   If you require a username and password the Database Connection URL format for the Informix JDBC driver is:

   jdbc:informix-sqli://<database hostname>:<tcp port><database server>:INFORMIXSERVER=<database>;user=myuser;password=mypassword

   For example to connect to the Database Server sysmaster running on the machine called pond.thiscompany.com and the Database called maindbase, you would use:

   jdbc:informix-sqli://pond.thiscompany.com:1526/sysmaster:INFORMIXSERVER=maindbase;

The **Database Driver** for the Informix JDBC driver is:

com.informix.jdbc.IfxDriver

Enter this string into the Database Driver text box under the Advanced Settings section of the Add Database Query Monitor form.

Monitoring MySQL Databases

Monitoring a MySQL database requires the use of a JDBC driver.

To enable SiteScope to monitor a MySQL database:

1. Download the JDBC driver from http://www.mysql.com/downloads/api-jdbc.html.
2. Uncompress the distribution file
3. Among all the other files, you should find a file with a .jar extension.
4. Copy the .jar file into the **<SiteScope install path>/SiteScope/java/lib/ext** directory.
5. Stop and restart SiteScope.
6. Now, use your browser to add a Database Query Monitor within SiteScope.

   The Database Connection URL format for the MySQL JDBC driver is:

   jdbc:mysql://<database hostname>[:<tcp port>]/<database>

   For example to connect to the MySQL database "aBigDatabase" on a machine using the standard MySQL port number 3306 you would use:

   jdbc:mysql://206.168.191.19/aBigDatabase

   If you are using a different port to connect to the database then you should include that port number as part of the IP address.

   The specification for the MySQL JDBC driver is: org.gjt.mm.mysql.Driver

   Enter this string into the Database Driver text box under the Advanced Settings section of the Add Database Query Monitor form.

Possible errors using the MySQL Driver

If, after setting this up, you get an authorization error in the Database Query Monitor, then you may have to grant rights for the SiteScope machine to access the MySQL database. Consult the MySQL Database administrator for setting up privileges for the SiteScope machine to access the MySQL server.

Monitoring Sybase Databases

To use JDBC drivers with your Sybase SQL server, please following the following steps:

1. **Finding the driver:** Obtain the driver for the version of Sybase that you are using. For example, for version 5.X databases you will need jconn2.jar. If you have Jconnect, you should be able to find a driver in the Jconnect directory. Mercury Interactive does not provide the drivers. Most drivers can be downloaded from the internet.
2. **Where to put the driver:** Place the zip file in the **<SiteScope install path>\SiteScope\java\lib\ext** directory.

Note: Do not extract the zip file.

---

3. Stop and restart the SiteScope service
4. Add a Database Query Monitor in SiteScope
5. For the database connection use the syntax of:

   jdbc:sybase:Tds:hostname:port

   For example to connect to SQL server named bgsu97 listening on port 2408, you would enter:

   jdbc:sybase:Tds:bgsu97:2408

6. You can specify a database by using the syntax:

   jdbc:sybase:Tds:hostname:port#/database

   For example to connect to SQL server named bgsu97 listening on port 2408 and to the database of quincy, you would enter:

jdbc:sybase:Tds:bgsu97:2408/quincy

7 Enter a query string for a database instance and table in the Sybase database you want to monitor.

- For example, Sp_help should work and return something similar to: good, 0.06 sec, 27 rows, KIRK1 , dbo, user table
- Alternately, the query string select * from spt_ijdbc_mda should return something similar to:
  Monitor: good, 0.06 sec, 175 rows, CLASSFORNAME, 1, create table #tmp_class_for_name (xtbinaryoffrow image null), sp_ijdbc_class_for_name(?), select * from #tmp_class_for_name, 1, 7, 12000, -1

8 Enter the database user name and password.

9 For the Database driver, enter:

- com.sybase.jdbc.SybDriver (for Sybase version 4.x)
- com.sybase.jdbc2.jdbc.SybDriver (for Sybase version 5.x)

10 Click the Add Monitor button.

Possible Errors with the Sybase database Monitoring

- Verify you are using the correct driver for the version of Sybase you are monitoring. For example:
  com.sybase.jdbc2.jdbc.SybDriver is the driver for Sybase version 5.x
  com.sybase.jdbc.SybDriver is the driver for Sybase version 4.x
- If you get the error: error, driver connect error, com/sybase/jdbc/SybDriver, click edit for the monitor and verify that there are no spaces at the end of the driver name in the text box. Then save the changes and try the monitor again.
- If you get the error: connect error, JZ006: Caught IOException: java.net.UnknownHostException: dbservername, verify the name of the database server you have entered in the Database Connection URL box is correct.

24

DB2 Monitor

The DB2 Monitor allows you to monitor the availability and performance statistics of an IBM DB2 database versions 6.x and 7.x. The 8.x versions of DB2 is not currently supported. The error and warning thresholds for the monitor can be set on one or more DB2 server performance statistics.

This chapter describes:	On page:
About the DB2 Monitor	249
Configuring the DB2 Monitor	250

About the DB2 Monitor

Use the DB2 Monitor to monitor DB2 servers for availability and proper function. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate DB2 Monitor instance for each IBM DB2 server in your environment.

The following are several key requirements for using the DB2 Monitor:

- The DB2 client files and libraries must be copied to the machine where SiteScope is running. The DB2 client Control Center must be installed on the SiteScope server.
- In the DB2 Control Center console, the system you want to monitor must be added to the **Systems** list. In Add System dialog box, enter the information required:
- **System Name:** *<db2_server_name>*
- **Remote Instance:**DB2

- **Host Name:** <*db2_server_name*>
- **Service Name:** <*db2_server_port*> (the default is port 50000)

Click Retrieve and then click OK.

- A remote DB2 instance needs to be added to the <*db2_server_name*> node in the Control Center Console. Select the <*db2_server_name*> node and select to add and Instance. Enter the information required in the dialog box:
- **Remote Instance:** DB2
- **Instance Name:**<*database_name_used_for_DB2_monitor*>
- **Host Name:** <*db2_server_name*>
- **Service Name:** <*db2_server_port*> (the default is port 50000)

Then click OK.

The default run schedule for this monitor is every 10 minutes, but you can change it to run more or less often using the **Frequency** setting.

Configuring the DB2 Monitor

The DB2 Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the DB2 Monitor.

Main Settings for the DB2 Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the IBM DB2 database system, how often this DB2 Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this DB2 monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the DB2 Monitor should DB2 system check the IBM DB2 database system. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Server

Enter the address or name of the server where the DB2 database is running.

Node Name

Enter the DB2 database node name that you want to monitor. For example, DB2 is a default node created by DB2 installation.

Username

Enter the DB2 database username to be used to access the DB2 server. This is usually a DB2 administrator username.

Password

Enter the password for the user specified above.

Counters

You use the features associated with the **Counters** setting to choose and manage the metrics you want to monitor with the DB2 Monitor. Use the following steps to select and add counters.

To select or add counters:

1. Click **Get Counters** to query the remote system. After SiteScope has successfully connected to the remote system, the Get Counters selection dialogue opens.
2. Use the features in the Get Counters selection dialogue screen to select the IBM DB2 database system metrics you want to monitor. Use the expandable menu controls as applicable to browse the available counters.

3 Use the check boxes to select between one and ten counters to be monitored.

4 Click **OK** to add the selected counters to the monitor configuration. The Get Counters selection dialogue closes and the monitor properties are updated with your selection.

Use the following steps to remove a counter from the selected counters list.

To remove or edit counters:

1 Click to edit the monitor for which you want to remove counters. Alternately, you may select the monitor you want to edit and click the Properties tab and click the **Edit** button. The monitor Properties screen opens.

2 Click the **Get Counters** button to open the Get Counters selection dialogue.

3 Clear the check box to the left of the current counter you want to remove.

At this point, you may add other counters to the monitor by clicking the applicable check boxes.

4 Click **OK** at the bottom of the screen to update the monitor.

The performance parameters or counters available for the DB2 Monitor are included in the table in the next section.

Counters Available for the DB2 Monitor

rem_cons_in	direct_read_time	pool_read_time
rem_cons_in_exec	direct_write_time	prefetch_wait_time
local_cons	cat_cache_lookups	pool_data_to_estore
local_cons_in_exec	cat_cache_inserts	pool_index_to_estore
con_local_dbases	cat_cache_overflows	pool_data_from_estore
agents_registered	cat_cache_heap_full	pool_index_from_estore
agents_waiting_on_token	pkg_cache_lookups	direct_reads
idle_agents	pkg_cache_inserts	direct_writes

agents_from_pool	pkg_cache_num_overflows	direct_read_reqs
agents_created_empty_pool	appl_section_lookups	direct_write_reqs
agents_stolen	appl_section_inserts	direct_read_time
comm_private_mem	sec_logs_allocated	direct_write_time
inactive_gw_agents	log_reads	cat_cache_lookups
num_gw_conn_switches	log_writes	cat_cache_inserts
sort_heap_allocated	total_log_used	cat_cache_overflows
post_threshold_sorts	locks_held	cat_cache_heap_full
piped_sorts_requested	lock_list_in_use	pkg_cache_lookups
piped_sorts_accepted	deadlocks	pkg_cache_inserts
appls_cur_cons	lock_escals	appl_section_lookups
appls_in_db2	x_lock_escals	appl_section_inserts
total_sec_cons	lock_timeouts	uow_log_space_used
num_assoc_agents	lock_waits	locks_held
sort_heap_allocated	lock_wait_time	deadlocks
total_sorts	locks_waiting	lock_escals
total_sort_time	rows_deleted	x_lock_escals
sort_overflows	rows_inserted	lock_timeouts
active_sorts	rows_updated	lock_waits
total_hash_joins	rows_selected	lock_wait_time
total_hash_loops	int_rows_deleted	locks_waiting
hash_join_overflows	int_rows_updated	uow_lock_wait_time
hash_join_small_overflows	int_rows_inserted	rows_deleted
pool_data_l_reads	static_sql_stmts	rows_inserted

pool_data_p_reads	dynamic_sql_stmts	rows_updated
pool_data_writes	failed_sql_stmts	rows_selected
pool_index_l_reads	commit_sql_stmts	rows_written
pool_index_p_reads	rollback_sql_stmts	rows_read
pool_index_writes	select_sql_stmts	int_rows_deleted
pool_read_time	uid_sql_stmts	int_rows_updated
pool_write_time	ddl_sql_stmts	int_rows_inserted
files_closed	int_auto_rebinds	open_rem_curs
pool_async_data_reads	int_commits	open_rem_curs_blk
pool_async_data_writes	int_rollbacks	rej_curs_blk
pool_async_index_writes	int_deadlock_rollbacks	acc_curs_blk
pool_async_index_reads	binds_precompiles	open_loc_curs
pool_async_read_time	agents_stolen	open_loc_curs_blk
pool_async_write_time	num_assoc_agents	static_sql_stmts
pool_async_data_read_reqs	total_sorts	dynamic_sql_stmts
pool_lsn_gap_clns	total_sort_time	failed_sql_stmts
pool_drty_pg_steal_clns	sort_overflows	commit_sql_stmts
pool_drty_pg_thrsh_clns	total_hash_joins	rollback_sql_stmts
prefetch_wait_time	total_hash_loops	select_sql_stmts
pool_data_to_estore	hash_join_overflows	uid_sql_stmts
pool_index_to_estore	hash_join_small_overflows	ddl_sql_stmts

pool_data_from_estore	pool_data_l_reads	int_auto_rebinds
pool_index_from_estore	pool_data_p_reads	int_commits
direct_reads	pool_data_writes	int_rollbacks
direct_writes	pool_index_l_reads	int_deadlock_rollbacks
direct_read_reqs	pool_index_p_reads	binds_precompiles
direct_write_reqs	pool_index_writes	

Advanced Settings for the DB2 Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the DB2 Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set one or more status thresholds criteria for each status condition per monitor instance. The status of the monitor and any associated alert action will be set based on comparison of all the threshold criteria you define for the monitor. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the DB2 or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the DB2 Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

25

DB2 8.x Monitor

The SiteScope DB2 Monitor allows you to monitor the availability and performance statistics of an IBM DB2 database for versions 8.x. The error and warning thresholds for the monitor can be set on as many as ten DB2 server performance statistics.

This chapter describes:	On page:
About the DB2 8.x Monitor	261
Configuring the DB2 8.x Monitor	262

About the DB2 8.x Monitor

Use the DB2 Monitor to monitor DB2 servers for availability and proper functioning. You can monitor multiple parameters or counters with a single monitor instance. This allows you to monitor server loading for performance, availability, and capacity planning. Create a separate DB2 Monitor instance for each Database in your IBM DB2 environment.

The following are several key requirements for using the DB2 Monitor:

- JDBC drivers for connecting to the DB2 Database server. These can be found in your DB2 server installation directories. You must use the following files: db2jcc_license_cu.jar, db2jcc_license_cisuz.jar, db2jcc.jar.
- This monitor uses the Snapshot mirroring functionality supported by DB2. You must enable the Snapshot Mirror on your DB2 instance to retrieve counters. See the following information from the IBM DB2 documentation: http://www-128.ibm.com/developerworks/db2/library/techarticle/dm-0408hubel/

The default run schedule for this monitor is every 10 minutes, but you can modify the monitor to run more or less often using the Update every setting.

Configuring the DB2 8.x Monitor

The DB2 8.x Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the DB2 8.x Monitor.

Main Settings for the DB2 8.x Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the IBM DB2 database system, how often this DB2 8.x Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this DB2 8.x monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the DB2 8.x Monitor should DB2 system check the IBM DB2 database system. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Server

Enter the address or name of the server where the DB2 8.x database is running.

Node Name

Enter the DB2 database node name that you want to monitor. For example, DB2 is a default node created by DB2 installation.

Username

Enter the DB2 database username to be used to access the DB2 server. This is usually a DB2 administrator username.

Password

Enter the password for the user specified above.

Counters

You use the features associated with the **Counters** setting to choose and manage the metrics you want to monitor with the DB2 8.x Monitor. Use the following steps to select and add counters.

To select or add counters:

1. Click **Get Counters** to query the remote system. After SiteScope has successfully connected to the remote system, the Get Counters selection dialogue opens.
2. Use the features in the Get Counters selection dialogue screen to select the IBM DB2 database system metrics you want to monitor. Use the expandable menu controls as applicable to browse the available counters.
3. Use the check boxes to select between one and ten counters to be monitored.
4. Click **OK** to add the selected counters to the monitor configuration. The Get Counters selection dialogue closes and the monitor properties are updated with your selection.

Use the following steps to remove a counter from the selected counters list.

To remove or edit counters:

1. Click to edit the monitor for which you want to remove counters. Alternately, you may select the monitor you want to edit and click the Properties tab and click the **Edit** button. The monitor Properties screen opens.

2 Click the **Get Counters** button to open the Get Counters selection dialogue.

3 Clear the check box to the left of the current counter you want to remove.

At this point, you may add other counters to the monitor by clicking the applicable check boxes.

4 Click **OK** at the bottom of the screen to update the monitor.

The performance parameters or counters available for the DB2 Monitor are included in the table in the next section.

Counters Available for the DB2 8.x Monitor

rem_cons_in	direct_read_time	pool_read_time
rem_cons_in_exec	direct_write_time	prefetch_wait_time
local_cons	cat_cache_lookups	pool_data_to_estore
local_cons_in_exec	cat_cache_inserts	pool_index_to_estore
con_local_dbases	cat_cache_overflows	pool_data_from_estore
agents_registered	cat_cache_heap_full	pool_index_from_estore
agents_waiting_on_token	pkg_cache_lookups	direct_reads
idle_agents	pkg_cache_inserts	direct_writes
agents_from_pool	pkg_cache_num_overflows	direct_read_reqs
agents_created_empty_pool	appl_section_lookups	direct_write_reqs
agents_stolen	appl_section_inserts	direct_read_time
comm_private_mem	sec_logs_allocated	direct_write_time
inactive_gw_agents	log_reads	cat_cache_lookups
num_gw_conn_switches	log_writes	cat_cache_inserts
sort_heap_allocated	total_log_used	cat_cache_overflows
post_threshold_sorts	locks_held	cat_cache_heap_full
piped_sorts_requested	lock_list_in_use	pkg_cache_lookups

piped_sorts_accepted	deadlocks	pkg_cache_inserts
appls_cur_cons	lock_escals	appl_section_lookups
appls_in_db2	x_lock_escals	appl_section_inserts
total_sec_cons	lock_timeouts	uow_log_space_used
num_assoc_agents	lock_waits	locks_held
sort_heap_allocated	lock_wait_time	deadlocks
total_sorts	locks_waiting	lock_escals
total_sort_time	rows_deleted	x_lock_escals
sort_overflows	rows_inserted	lock_timeouts
active_sorts	rows_updated	lock_waits
total_hash_joins	rows_selected	lock_wait_time
total_hash_loops	int_rows_deleted	locks_waiting
hash_join_overflows	int_rows_updated	uow_lock_wait_time
hash_join_small_overflows	int_rows_inserted	rows_deleted
pool_data_l_reads	static_sql_stmts	rows_inserted
pool_data_p_reads	dynamic_sql_stmts	rows_updated
pool_data_writes	failed_sql_stmts	rows_selected
pool_index_l_reads	commit_sql_stmts	rows_written
pool_index_p_reads	rollback_sql_stmts	rows_read
pool_index_writes	select_sql_stmts	int_rows_deleted
pool_read_time	uid_sql_stmts	int_rows_updated
pool_write_time	ddl_sql_stmts	int_rows_inserted
files_closed	int_auto_rebinds	open_rem_curs
pool_async_data_reads	int_commits	open_rem_curs_blk

pool_async_data_writes	int_rollbacks	rej_curs_blk
pool_async_index_writes	int_deadlock_rollbacks	acc_curs_blk
pool_async_index_reads	binds_precompiles	open_loc_curs
pool_async_read_time	agents_stolen	open_loc_curs_blk
pool_async_write_time	num_assoc_agents	static_sql_stmts
pool_async_data_read_reqs	total_sorts	dynamic_sql_stmts
pool_lsn_gap_clns	total_sort_time	failed_sql_stmts
pool_drty_pg_steal_clns	sort_overflows	commit_sql_stmts
pool_drty_pg_thrsh_clns	total_hash_joins	rollback_sql_stmts
prefetch_wait_time	total_hash_loops	select_sql_stmts
pool_data_to_estore	hash_join_overflows	uid_sql_stmts
pool_index_to_estore	hash_join_small_overflows	ddl_sql_stmts
pool_data_from_estore	pool_data_l_reads	int_auto_rebinds
pool_index_from_estore	pool_data_p_reads	int_commits
direct_reads	pool_data_writes	int_rollbacks
direct_writes	pool_index_l_reads	int_deadlock_rollbacks
direct_read_reqs	pool_index_p_reads	binds_precompiles
direct_write_reqs	pool_index_writes	

Advanced Settings for the DB2 8.x Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the DB2 8.x Monitor and its display in the product interface. See

"Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set one or more status thresholds criteria for each status condition per monitor instance. The status of the monitor and any associated alert action will be set based on comparison of all the threshold criteria you define for the monitor. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the DB2 8.x or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1 Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.

2 Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.

3 Enter a value applicable to the measurement parameter in the third text box.

4 To add another threshold setting, click the **New Error If** button and repeat the steps above.

5 Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the DB2 8.x Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see “Common Monitor Settings” in the chapter Chapter 2, “Working with SiteScope Monitors.”

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see “Working with Categories” in *Working with Monitor Administration*.

26

Disk Space Monitor

The Disk Space Monitor provides a tool for you to track how much disk space is currently in use on your server. A full disk can cause a host of problems including system crashes and corrupt files.

This chapter describes:	On page:
About the Disk Space Monitor	273
Configuring the Disk Space Monitor	274

About the Disk Space Monitor

What to Monitor

Running out of disk space can cause a host of problems both large and small, and it is something that can happen slowly over time or very rapidly. Having SiteScope verify that your disk space is within acceptable limits can save you from a crashed system and corrupted files.

About Scheduling this Monitor

The disk space monitor does not require many resources, so you can check it as often as every 15 seconds, but every 10 minutes should be sufficient. You can specify both warning and error thresholds so that SiteScope can notify you of a potential problem in time for you to do something about it. You may even want to have SiteScope execute a script (using a Script Alert) that deletes all files in certain directories, such as /tmp, when disk space becomes constrained.

Configuring the Disk Space Monitor

The Disk Space Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the Disk Space Monitor.

Main Settings for the Disk Space Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the remote disk drive, how often this Disk Space Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this Disk Space monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the Disk Space Monitor should disk space check the remote disk drive. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Server

Choose the server for which you want to monitor Disk Space. The default is to monitor disks on the server on which SiteScope is installed. Use the drop-down list to select a server from the list of remote servers that are available to the SiteScope agent.

Disk

Select the disk drive that you want to monitor from the list.

Note: Disk performance counters are disabled by default in standard Windows 2000 installations. In order for you to monitor disk drives using the SiteScope Disk Monitor on servers running Windows 2000, you must enable these disk counters. Use the diskperf -y command line on each Win2000 machine you want to monitor disk space and then reboot each server. You should then be able to select the disk drives for those servers in the SiteScope Disk Monitor form.

Advanced Settings for the Disk Space Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Disk Space Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set up to ten status thresholds criteria for each status condition per monitor instance. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the Disk Space or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the Disk Space Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

27

Directory Monitor

The Directory Monitor watches an entire directory and reports on the total number of files in the directory, the total amount of disk space used, and the time (in minutes) since any file in the directory was modified. This information is useful if you have limited disk space, you want to monitor the number of files written to a specific directory, or you want to know the activity level in a certain directory.

This chapter describes:	On page:
About the Directory Monitor	281
Configuring the Directory Monitor	282

About the Directory Monitor

The Directory Monitor is very useful for watching directories that contain log files or other files that tend to grow and multiply unpredictably. You can instruct SiteScope to notify you if either the number of files or total disk space used gets out of hand.

What to Monitor

Use this monitor to watch directories that contain files that may grow large enough to cause disk space problems. You can also use this to monitor directories in which new files are added and deleted frequently. A good example of the latter is an FTP directory. In the case of an FTP directory, you will probably want to watch both the number files in the directory and the files contained in the directory.

About Scheduling This Monitor

Because the uses for the Directory Monitor vary so greatly there is no one interval that works best. Keep in mind that if you are watching a directory that contains a lot of files and sub directories, this monitor may take longer to run.

Configuring the Directory Monitor

The Directory Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the Directory Monitor.

Main Settings for the Directory Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the remote directory, how often this Directory Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this Directory monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the Directory Monitor should directory check the remote directory. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Directory Path

Enter the directory that you want to monitor. To monitor a directory on a remote machine in a Windows NT/2000 network, enter the UNC name for that directory. For example, \\server\directory\subdirectory.

If you want to monitor a directory that is created automatically by some application and the directory path includes date or time information, you can use SiteScope's special data and time substitution variables in the path name of the directory.

You can also monitor directories on a remote Windows NT/2000 server through NetBIOS by including the UNC path to the remote directory. For example, \\remoteserver\sharedfolder\targetdirectory. This requires that the user account under which SiteScope is running has permission to access the remote directory using the UNC path. If a direct connection via the operating system is unsuccessful, SiteScope will try to match the \\remoteserver with servers currently defined remote NT connection profiles (displayed in the Remote NT Servers table). If an exact match is found \\remoteserver in the remote NT connection profiles, SiteScope will try to use this connection profile to access the remote directory. If no matching server name is found, the monitor reports that the remote directory can not be found.

Advanced Settings for the Directory Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Directory Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

No Subdirectories

Check this box if you do not want SiteScope to count subdirectories.

File Name Match

Optional, enter text or an expression to match against. Only filenames which match will be counted in the totals.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule

➤ Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set up to ten status thresholds criteria for each status condition per monitor instance. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the Directory or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the Directory Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

28

DHCP Monitor

The DHCP Monitor checks a DHCP Server via the network. It verifies that the DHCP server is listening for requests and that it can allocate an IP address in response to a request.

This chapter describes:	On page:
About the DHCP Monitor	289
Installation of DHCP Software Library	290
Configuring the DHCP Monitor	290

Note: This monitor requires that a third-party Java DHCP library be installed on the server where SiteScope is running. The DHCP Monitor type will not appear in the interface until this library is installed. See the section on Installation of DHCP Software Library below for more information.

About the DHCP Monitor

If your DHCP server fails, machines relying on DHCP will be unable to acquire a network configuration when rebooting. Additionally, as DHCP address leases expire on already-configured machines, those machines will "drop off" the network when the DHCP server fails to renew their address lease. Therefore, it is important that you monitor your DHCP server(s) to verify that they are working properly.

Most networks have a DHCP server listening for DHCP requests. This monitor will "find" DHCP servers by broadcasting a request for an IP address and waiting for a DHCP server to respond.

About Scheduling This Monitor

Each time the DHCP Monitor runs, it returns a status and writes it in the monitoring log file. It also writes the total time it takes to receive and release an IP address in the log file.

Your DHCP server is a critical part of providing functionality to other hosts on your network, so it should be monitored frequently (every 2-5 minutes).

Installation of DHCP Software Library

The SiteScope DHCP Monitor uses the jDHCP library, available from http://www.dhcp.org/javadhcp/. After downloading the library (either in .zip or in .tar.gz format), extract the file named JDHCP.jar and place it in the **<SiteScope install path>/SiteScope/java/lib/ext** directory, such that the file is located at **<SiteScope install path>/SiteScope/java/lib/ext/JDHCP.jar**. After installing the JDHCP.jar file, stop and restart the SiteScope service. The DHCP Monitor will not be usable until the jDHCP library is installed and SiteScope has been restarted.

Configuring the DHCP Monitor

The DHCP Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the DHCP Monitor.

Main Settings for the DHCP Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the DHCP server, how often this DHCP Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this DHCP monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the DHCP Monitor should DHCP request the DHCP server. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Timeout

Enter the time, in seconds, to wait for an IP address.

Advanced Settings for the DHCP Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the DHCP Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Requested Client Address

Optionally, the IP address to request from the DHCP server.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule

➤ Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set up to ten status thresholds criteria for each status condition per monitor instance. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the DHCP or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the DHCP Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

29

DNS Monitor

The DNS Monitor checks a Domain Name Server via the network. It verifies that the DNS server is accepting requests, and also verifies that the address for a specific domain name can be found.

Each time the DNS Monitor runs, it returns a status and writes it in the monitoring log file.

This chapter describes:	On page:
About the DNS Monitor	297
Configuring the DNS Monitor	298

About the DNS Monitor

If your DNS server is not working properly, you will not be able to get out on the network and people trying to reach your server will not be able to find it. Therefore, it is important that you monitor your DNS server(s) to check that they are working properly.

Most companies have both a primary and a secondary DNS server. If your company employs a firewall, these servers may sit outside the firewall with another DNS server located inside the firewall. This internal DNS server provides domain name service for internal machines. It is important to monitor all of these servers to check that each is functioning properly.

About Scheduling This Monitor

If your DNS servers fail, users will start complaining that "everything's broken", so you should monitor them often. For example, assume that you have both a primary and secondary DNS server outside your firewall and an internal DNS server inside your firewall. Your internal server is critical, so you should monitor that one every 2 - 5 minutes. That's also a good interval for your primary DNS server that sits outside of your firewall. You can monitor the secondary DNS server less often. Every 10 or 15 minutes should be fine.

Configuring the DNS Monitor

The DNS Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the DNS Monitor.

Main Settings for the DNS Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the Domain Name Server, how often this DNS Monitor instance should be run, and the text name used for this monitor instance. See “Common Monitor Settings” in the chapter “Working with SiteScope Monitors” for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this DNS monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the DNS Monitor should DNS system check the Domain Name Server. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Server Address

Enter the IP address of the DNS server that you want to monitor (for example, 206.168.191.1).

Host Name

Enter the host name to lookup (for example, demo.thiscompany.com). If you only want to verify that your DNS server is operating, the host name you enter here can be any valid host name or domain name. To verify that a domain name resolves to a specific IP address, enter the IP address that corresponds to the host name you enter in the **Host address** box in the Advanced Settings section below.

Advanced Settings for the DNS Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the DNS Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Host address

Optionally, you can use the DNS monitor to verify that a host name or domain name resolves to the correct IP address or addresses. Enter the IP address or addresses that are mapped to the **Host Name** (domain name) entered above.

Note: If you enter more than one IP address, the monitor will report a status of good, even if only one of the IP addresses that you enter is mapped correctly to the **Host Name** . When using this option, the monitor only reports an error if none of the IP addresses entered in this field are mapped to the given **Host Name**.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set up to ten status thresholds criteria for each status condition per monitor instance. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the DNS or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.

3 Enter a value applicable to the measurement parameter in the third text box.

4 To add another threshold setting, click the **New Error If** button and repeat the steps above.

5 Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the DNS Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

30

Dynamo Application Server Monitor

The SiteScope Dynamo Application Server Monitor allows you to monitor the availability of an ATG Dynamo platform. The error and warning thresholds for the monitor can be set on one or more Dynamo Application Server Monitor performance statistics via SNMP.

This chapter describes:	On page:
About the Dynamo Application Server Monitor	305
Configuring the Dynamo Application Server Monitor	306

About the Dynamo Application Server Monitor

Use the Dynamo Application Server Monitor to monitor the server performance data for ATG Dynamo servers using SNMP. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate monitor instance for each ATG Dynamo server in your environment.

The default run schedule for this monitor is every 10 minutes, but you can change it to run more or less often using the **Frequency** setting.

Configuring the Dynamo Application Server Monitor

The Dynamo Application Server Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the Dynamo Application Server Monitor.

Main Settings for the Dynamo Application Server Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the ATG Dynamo system, how often this Dynamo Application Server Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this Dynamo Application Server monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the Dynamo Application Server Monitor should system check the ATG Dynamo system. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Host Name

Enter the IP address or host name of the Dynamo Server to be monitored along with the port that server is answering on. The default port is 8870. If the SNMP agent for the Dynamo server is answering on a different port, you must include the port number as part of the host name address.

Counters

Select the server performance parameters or counters you want to check with this monitor. The table list to the right of this item displays those currently selected for this monitor. Click **Get Counters** to bring up the counters selection screen. Check or clear the check boxes on the Get Counters screen to select one or more counters to monitor on this server. The performance parameters or counters available (with corresponding OID) for the Dynamo Application Server Monitor include:

sysTotalMem:1.3.6.1.4.1.2725.1.1.4
sysFreeMem:1.3.6.1.4.1.2725.1.1.5
sysNumInfoMsgs:1.3.6.1.4.1.2725.1.1.6
sysNumWarningMsgs:1.3.6.1.4.1.2725.1.1.7
sysNumErrorMsgs:1.3.6.1.4.1.2725.1.1.8
lmlsManager:1.3.6.1.4.1.2725.1.2.1
lmManagerIndex:1.3.6.1.4.1.2725.1.2.2
lmlsPrimaryManager:1.3.6.1.4.1.2725.1.2.3
lmServicingCMs:1.3.6.1.4.1.2725.1.2.4
lmCMLDRPPort:1.3.6.1.4.1.2725.1.2.6
dbIndex:1.3.6.1.4.1.2725.1.5.1.1.1.1
dbMinConn:1.3.6.1.4.1.2725.1.5.1.1.3.1
dbMaxConn:1.3.6.1.4.1.2725.1.5.1.1.4.1
dbMaxFreeConn:1.3.6.1.4.1.2725.1.5.1.1.5.1
dbBlocking:1.3.6.1.4.1.2725.1.5.1.1.6.1
dbConnOut:1.3.6.1.4.1.2725.1.5.1.1.7.1
dbFreeResources:1.3.6.1.4.1.2725.1.5.1.1.8.1
dbTotalResources:1.3.6.1.4.1.2725.1.5.1.1.9.1
drpPort:1.3.6.1.4.1.2725.1.4.2
drpTotalReqsServed:1.3.6.1.4.1.2725.1.4.3

drpTotalReqTime:1.3.6.1.4.1.2725.1.4.4
drpAvgReqTime:1.3.6.1.4.1.2725.1.4.5
drpNewSessions:1.3.6.1.4.1.2725.1.4.6
drpAvailable:1.3.6.1.4.1.2725.1.4.7
stCreatedSessionCnt:1.3.6.1.4.1.2725.1.3.1
stValidSessionCnt:1.3.6.1.4.1.2725.1.3.2
stRestoredSessionCnt:1.3.6.1.4.1.2725.1.3.3
stDictionaryServerStatus:1.3.6.1.4.1.2725.1.3.4

Index

Enter the index of the SNMP object you want to check with this monitor. Non-table object IDs have an index of 0 (zero).

Community

Enter the community that the above SNMP object belongs to. The default community is public. You may need to consult with your network administrators about what community names are active in your network environment

Advanced Settings for the Dynamo Application Server Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Dynamo Application Server Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Retry Delay

Enter the time, in seconds, that SiteScope should wait before retrying a request.

Timeout

Enter the total time, in seconds, that SiteScope should wait for a successful reply from the Dynamo server. If a reply is not received in the time indicated, the monitor returns a timeout error.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set one or more status thresholds criteria for each status condition per monitor instance. The status of the monitor and any associated alert action will be set based on comparison of all the threshold criteria you define for the monitor. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the Dynamo Application Server or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1 Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.

2 Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.

3 Enter a value applicable to the measurement parameter in the third text box.

4 To add another threshold setting, click the **New Error If** button and repeat the steps above.

5 Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the Dynamo Application Server Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see “Common Monitor Settings” in the chapter Chapter 2, “Working with SiteScope Monitors.”

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see “Working with Categories” in *Working with Monitor Administration*.

31

eBusiness Chain Monitor

You use the eBusiness Chain Monitor to verify the multiple tasks that make up an online transaction are completed properly, ensuring end-to-end transaction success. This may include successful navigation through a series of URLs, transmission of an e-mail confirming the sequence, and logging the information into a database file. This monitor runs a sequence of other SiteScope monitors, checking that each monitor returns a status of OK. If any monitor in the sequence fails, the eBusiness Chain Monitor reports an Error status.

This chapter describes:	On page:
About the eBusiness Chain Monitor	315
Setting up Monitors for the eBusiness Chain	317
Configuring the eBusiness Chain Monitor	318
Passing Values from One Monitor to Another	324

About the eBusiness Chain Monitor

Use this monitor to verify that an end-to-end transaction and associated processes complete properly. For example, you could use this monitor to verify that the following steps, each of which is a step in a single transaction, execute properly:

- Place an order on a Web site (URL Sequence monitor)
- Check that the order status was updated (URL Sequence monitor)
- Check that a confirmation e-mail was received (Mail monitor)

- Check that the order was added to the order database (Database monitor)
- Check that the order was transferred to a legacy system (Script monitor or Custom monitor)

You should monitor any multi-step transaction process that causes other updates or actions in your systems. Monitor each of the actions taken to check that updates were performed properly and that actions were carried out successfully.

Using this example, you would first create the URL Sequence monitor, Mail monitor, Database monitor, and applicable Script monitor needed to verify each step of the chain. Then you would create an eBusiness Chain Monitor and select each of these SiteScope monitors as a group in the order they should be executed. If any one monitor indicates a failure, the eBusiness Chain Monitor will report an error.

Editing the Order of the Monitors in the Chain

By default, Add eBusiness Chain Monitor page will list monitor groups and individual monitors in the order they are created. To have the eBusiness Chain Monitor invoke the chain of monitors in the proper order, they will need to appear in the proper order in the selection menu on the Add eBusiness Chain Monitor page. You can do this by creating the individual monitors in the order which they should be executed (see Setup section below). You can also use the "Reorder the monitors in this group" option on the Monitor Group page.

About Scheduling This Monitor

Each time the eBusiness Chain Monitor runs, it returns a status based upon the number and percentage of items in the specified monitors and/or groups currently reporting an error, warning, or OK status. It writes the percentages reported in the monitoring log file.

The general rule of thumb is to run these monitors every 10 minutes or so. If you have a very critical transaction process, you may want to run them more often.

Setting up Monitors for the eBusiness Chain

Before you can add an eBusiness Chain Monitor, you will need to define other SiteScope monitors that will report on the actions and results of the steps in the sequence chain. Using the example from the usage guidelines above, you might create one or more URL Sequence monitors for verifying the sequence of online actions, a mail monitor to confirm that an e-mail acknowledgement is sent, and a Database Query monitor to see that information entered online is logged into a database. To facilitate administration, use the following steps to set up a URL sequence chain monitor:

1. Create a new group that will contain all the individual monitors to be included in the sequence chain.
2. Open the new monitor group.
3. Add the first individual monitor type needed to for the sequence (e.g URL Sequence Monitor).

Note: Monitors should be added in the order that they should be executed in the chain. For example, create a URL Sequence Monitor which will trigger an e-mail event **before** you create the Mail Monitor to check for the e-mail. See the note on reordering monitors above.

---

4. If necessary, set up the values to be passed from one monitor to another in the chain. For information about how this works see the section on passing variables between monitors below.
5. Add the other monitors for this transaction chain in the appropriate order of execution into the group.

Note: The individual monitors executed by the eBusiness Chain Monitor should generally not be run separately by SiteScope. You should make sure that the **Update Every** setting for each of these monitors is blank.

---

6 Return to the SiteScope main panel.

7 Create a new group or open an existing group that will contain the e-business transaction chain monitor you are creating.

8 Select the "Add a new monitor to the group" option and select the eBusiness Chain Monitor.

9 Complete the eBusiness Chain Monitor Form as described below .

Configuring the eBusiness Chain Monitor

The eBusiness Chain Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the eBusiness Chain Monitor.

Main Settings for the eBusiness Chain Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the online systems, how often this eBusiness Chain Monitor instance should be run, and the text name used for this monitor instance. See “Common Monitor Settings” in the chapter “Working with SiteScope Monitors” for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this eBusiness Chain monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the eBusiness Chain Monitor should transaction chain the online systems. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Items

Using the control key or equivalent, click the group or set of monitors that will make up the eBusiness Chain Monitor. As noted in the set up section above, the monitors are run in the order that they are listed in their group.

Advanced Settings for the eBusiness Chain Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the eBusiness Chain Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

When Error

Choose how you want errors during the sequence to be handled.

- Continue, run the remaining monitors - runs every monitor no matter what the status of a given monitor is
- Stop, do not run any of the remaining monitors - stops running the list of monitors immediately, if a monitor returns an error
- Run the last monitor - run the last monitor in the list, which is useful if a monitor is used for closing or logging off of a session opened in a previous monitor.

Single Session

Check this box if you want any URL monitors to use the same network connection and the same set of cookies. This is useful if you are using the eBusiness Chain Monitor to group several URL Sequence monitors and do not want to include the login steps as part of each transaction

Monitor Delay

Enter a number of seconds to wait between running each monitor. This setting is useful if you need to wait for processing to occur on your systems before running the next monitor.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule

➤ Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set up to ten status thresholds criteria for each status condition per monitor instance. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the eBusiness Chain or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the applicable monitor type Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

Passing Values from One Monitor to Another

You can pass values between individual monitors in an eBusiness Chain Monitor by using an extension of SiteScope's substitution syntax.

For example, to pass the matching value from a URL Monitor to the Receive Content Match box of a Mail Monitor, you would enter:

Receive Content Match: s|$value-step2.matchValue$|

where the "s| |" indicates that this should be treated as a substitution, "$value-xxxx$" means to retrieve the value from another monitor, "step2" means that the value should be retrieved from the second step of eBusiness Chain Monitor, and "matchValue" means get the matching value from that monitor.

A complete list of terms like "matchValue" can be found in the chapter on Template Properties in the SiteScope Reference Guide.

32

F5 Big-IP Monitor

The F5 Big-IP Monitor allows you to monitor the statistics of a F5 Big-IP load balancing device using SNMP. The error and warning thresholds for the monitor can be set on one or more load balancer statistics.

This chapter describes:	On page:
About the F5 Big-IP Monitor	325
Configuring the F5 Big-IP Monitor	325

About the F5 Big-IP Monitor

Use the F5 Big-IP Monitor to monitor the content of event logs and other data from F5 Big-IP load balancing device. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate F5 Big-IP monitor instance for each F5 Big-IP load balancing device in your environment.

The default run schedule for this monitor is every 10 minutes, but you can change it to run more or less often using the **Frequency** setting.

Configuring the F5 Big-IP Monitor

The F5 Big-IP Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the F5 Big-IP Monitor.

Main Settings for the F5 Big-IP Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the F5 Big-IP server, how often this F5 Big-IP Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this F5 Big-IP monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the F5 Big-IP Monitor should system check the F5 Big-IP server. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Server

Enter the name of the server you want to monitor.

MIB File

Select either the F5 MIB file or "All MIBs". Selecting the F5 MIB file will cause only those objects that are described within that MIB file to be displayed. Selecting "All MIBs" will cause all objects discovered on the given F5 Big-IP to be displayed when browsing counters. If no MIB information is available for an object, it is still displayed, but with no textual name or description.

SNMP Version

Select the version of SNMP to use when connecting.

Community

Enter the community string (valid only for version 1 or 2 connections).

SNMP V3 Authentication Type

Select the type of authentication to use for version 3 connections.

SNMP V3 Username

Enter the username for version 3 connections.

SNMP V3 Authentication Password

Enter the authentication password to use for version 3 connections.

SNMP V3 Privacy Password

Enter the privacy password if DES privacy encryption is desired for version 3 connections. Leave blank if you do not want privacy.

SNMP V3 Context Engine ID

Enter a hexadecimal string representing the Context Engine ID to use for this connection. This is applicable for SNMP V3 only.

SNMP V3 Context Name

Enter the Context Name to use for this connection. This is applicable for SNMP V3 only.

Counters

You use the features associated with the **Counters** setting to choose and manage the metrics you want to monitor with the F5 Big-IP Monitor. Use the following steps to select and add counters.

To select or add counters:

1. Click **Get Counters** to query the remote system. After SiteScope has successfully connected to the remote system, the Get Counters selection dialogue opens.
2. Use the features in the Get Counters selection dialogue screen to select the F5 Big-IP server metrics you want to monitor. Use the expandable menu controls as applicable to browse the available counters.
3. Use the check boxes to select between one and ten counters to be monitored.
4. Click **OK** to add the selected counters to the monitor configuration. The Get Counters selection dialogue closes and the monitor properties are updated with your selection.

Use the following steps to remove a counter from the selected counters list.

To remove or edit counters:

1. Click to edit the monitor for which you want to remove counters. Alternately, you may select the monitor you want to edit and click the Properties tab and click the **Edit** button. The monitor Properties screen opens.
2. Click the **Get Counters** button to open the Get Counters selection dialogue.
3. Clear the check box to the left of the current counter you want to remove.

   At this point, you may add other counters to the monitor by clicking the applicable check boxes.
4. Click **OK** at the bottom of the screen to update the monitor.

   The performance parameters or counters available for the F5 Big-IP Monitor include:

   - pktsin
   - pksout
   - concur
   - portdeny
   - uptime
   - droppedin
   - droppedout
   - MemoryUsed

Advanced Settings for the F5 Big-IP Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the F5 Big-IP Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Port

Enter the port to use when requesting data from the SNMP agent. The default of 161 is the port on which an SNMP agent will typically be listening.

Counter Calculation Mode

Use this option to perform a calculation on objects of type Counter, Counter32, or Counter64. The available calculations are:

- a simple delta of the current value from the previous value, OR
- a rate calculation using the delta of current value from previous value, divided by the time elapsed between measurements

---

Note: This option only applies to the aforementioned object types. An SNMP by MIB Monitor that monitors Counter objects as well as DisplayString objects will only perform this calculation on the Counter objects.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set one or more status thresholds criteria for each status condition per monitor instance. The status of the monitor and any associated alert action will be set based on comparison of all the threshold criteria you define for the monitor. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the F5 Big-IP or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the F5 Big-IP Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

33

File Monitor

The File Monitor reads a specified file. In addition to checking the size and age of a file, the File Monitor can help you verify that the contents of files, either by matching the contents for a piece of text, or by checking to see if the contents of the file ever changes

This chapter describes:	On page:
About the File Monitor	335
Configuring the File Monitor	336

About the File Monitor

The File Monitor is useful for watching files that can grow too large and eat up disk space, such as log files. You can set up your File Monitors to watch for file size, setting a threshold at which you should be notified. You can even write scripts for SiteScope to execute that will automatically roll log files when they reach a certain size.

What to Monitor

You can create File Monitors for any files that you want to monitor for size, age, or content. As mentioned before, you can set thresholds in SiteScope, telling it when to notify you of a problem. Log files are very good candidates for monitoring because they're prone to suddenly growing in size and crashing machines. Other files that you may want to watch are Web pages that have important content that does not change often. SiteScope can alert you to unauthorized content changes so that you can correct them immediately.

About Scheduling this Monitor

The frequency with which you run File Monitors is strictly up to you. We suggest that you run them as often as every 10 minutes, but you can run them more often if you prefer.

Reading and Status

Each time the File Monitor runs, it returns a reading and a status and writes them in the monitoring log file. It also writes the file size and age into the log file.

The reading is the current value of the monitor. Possible values are:

- OK
- content match error
- file not found
- contents changed

An error status is returned if the current value of the monitor is anything other than OK.

Configuring the File Monitor

The File Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the File Monitor.

Main Settings for the File Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the remote file, how often this File Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this File monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the File Monitor should file check the remote file. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

File Name

Enter the name of the file to be monitored. For example, /pub/docs/mydoc.txt.

You can also monitor files on a remote Windows NT/2000 server through NetBIOS by including the UNC path to the remote file. For example, \\remoteserver\sharedfolder\filename.ext. This requires that the user account under which SiteScope is running has permission to access the remote file using the UNC path. If a direct connection via the operating system is unsuccessful, SiteScope will try to match the \\remoteserver with servers currently defined remote NT connection profiles (displayed in the Remote NT Servers container). If an exact match is found \\remoteserver in the remote NT connection profiles, SiteScope will try to use this connection profile to access the file. If no matching server name is found, the monitor reports that the file can not be found.

File Encoding

If the file content to be monitored uses an encoding that is different than the encoding used on server where SiteScope is running, enter the code page or encoding to use. Some examples of commonly used encodings are: Cp1252, Cp1251, Cp1256, Shift_JIS or EUC_JP. This may be necessary if the code page which SiteScope is using does not support the character sets used in the target file. This will enable SiteScope to match and display the encoded file content correctly.

Advanced Settings for the File Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the File Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Match Content

Enter a string of text to check for in the returned page. If the text is not contained in the page, the monitor will display "no match on content". The search is case sensitive. Remember that HTML tags are part of a text document, so include the HTML tags if they are part of the text you are searching for (for example, "<B> Hello</B> World"). This works for XML pages as well. You may also perform a regular expression match by enclosing the string in forward slashes, with an "i" after the trailing slash indicating case-insensitive matching. (for example, /href=Doc\d+\.html/ or /href=doc\d+\.html/i). If you want a particular piece of text to be saved and displayed as part of the status, use parentheses in a Perl regular expression. For example /Temperature: (\d+). This would return the temperature as it appears on the page and this could be used when setting an Error if or Warning if threshold.

Check for Content Changes

Unless this is set to "no content checking" (the default) SiteScope will record a checksum of the document the first time the monitor runs and then does a checksum comparison each subsequent time it runs. If the checksum changes, the monitor will have a status of "content changed error" and go into error. If you want to check for content changes, you will usually want to use "compare to saved contents".

The options for this setting are:

- **no content checking** - (default) SiteScope does not check for content changes
- **compare to last contents** - The new checksum will be recorded as the default after the initial error "content changed error" occurs, so the monitor will return to OK until the checksum changes again
- **compare to saved contents** - The checksum is a snapshot of a given page (retrieved either during the initial or a specific run of the monitor). If the contents change, the monitor will get a "content changed error" and will stay in error until the contents return to the original contents, or the snapshot is update by resetting the saved contents
- **reset saved contents** - Takes a new snapshot of the page and saves the resulting checksum on the first monitor run after this option is chosen. After taking the snapshot, the monitor will revert to "compare to saved contents" mode.

No Error on File Not Found

Check this box if you want this monitor to remain in GOOD status, if the file is not found.

Note: You must also set the 'Good if' Condition to 'status == 404'

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See “Common Monitor Settings” in the chapter “Working with SiteScope Monitors” for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set up to ten status thresholds criteria for each status condition per monitor instance. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the File or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the File Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

34

Formula Composite Monitor

The Formula Composite Monitor is designed to simplify the monitoring of complex network environments by checking the status readings of two SNMP, Script, Database Query, or Windows Performance Counter monitors and performing an arithmetic calculation on their results.

This chapter describes:	On page:
About the Formula Composite Monitor	345
Configuring the Formula Composite Monitor	347

About the Formula Composite Monitor

One reason you should use this monitor is if you have devices or systems in your network that return values which you want to combine in some way to produce a composite value. The following monitor types can be used to build a Formula Composite Monitor:

- Database Query Monitor
- Script Monitor
- SNMP Monitor
- Windows Performance Counter Monitor

If you need alert logic that is more complex than SiteScope's standard alerts will allow, you may be able to use the Formula Composite Monitor to a create custom alert behavior. For example, you have two parallel network devices that record network traffic but the values need to be combined to produce an overall figure of network traffic. This monitor may also be used to combine the results returned by scripts run on two different machines.

Each time the Formula Composite Monitor runs, it returns a status based upon the measurement results of the two subordinate monitors and the calculation specified for the composite monitor.

Notes and Limitations

You must create at least two individual Script, SNMP, Database Query or Windows Performance Counter monitor instances before you can set up a Formula Composite Monitor for those monitors.

The monitors you create for use with a Formula Composite monitor should be configured to return a single value per monitor. This is generally simple with SNMP monitors. Database Query and Script monitors should use queries and scripts that return a single value. For Windows Performance Counter monitors, you can use the (Custom Object) option for the **PerfMon Chart File** setting and then specify a single performance **Object**, **Counter**, and **Instance** (if applicable) in the Advanced Settings section of the monitor setup. If a subordinate monitor is configured to return more than one numeric measurement, only the first numeric measurement from that monitor instance will be used by the Formula Composite Monitor.

You should only use the Formula Composite monitor for calculations that you consider to be compatible data types. The monitor does not verify that the data returned by the subordinate monitors are compatible.

You can select two different types of monitors as subordinate monitors of a Formula Composite monitor. For example, one monitor may be a Script monitor and the other may be a Database Query monitor.

Moving any of the monitors being used by the Formula Composite Monitor will cause the composite monitor to report an error. If it is necessary to move either of the underlying monitors, recreate or edit the Formula Composite Monitor to select the monitor from its new location.

Configuring the Formula Composite Monitor

The Formula Composite Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the Formula Composite Monitor.

Main Settings for the Formula Composite Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the monitored systems, how often this Formula Composite Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this Formula Composite monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the Formula Composite Monitor should comparison or calculation the monitored systems. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Items

Choose two SNMP monitors, two Script monitors, two Database monitors, or two Windows Performance Counter monitors from the selection menu that the Formula Composite Monitor should operate on. You can select individual monitors and then click the right arrow to the right of the selection menu to move the monitor to the selection list on the right. Select the second monitor from the list on the left and click the right arrow to move the selection to the list on the right. You may also control-click two monitors on a single operation and click the right arrow to move them to the list on the right.

Operation

Select the arithmetic operation to be performed on the results of the two monitors selected above. For example: Add the results, Multiply the results of the two monitors, Subtract the results of the first from the second, Divide the second by the first, and so forth.

Advanced Settings for the Formula Composite Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Formula Composite Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Run Monitors

Check this box if you want the Formula Composite Monitor to control the scheduling of the selected monitors, as opposed to just checking their status readings. This is useful if you want the monitors to run one after another or run at approximately the same time.

Note: Any monitors that are to be run this way should not also be run separately, so edit the individual monitors, blank out the **Update Every** box for that monitor, and save the changes. Those monitors will then only run when scheduled by the Formula Composite Monitor.

Monitor Delay

If Run Monitors is checked, this is the number of seconds to wait between running each monitor.

Constant

Enter an operator and a constant to operate on the result of the calculation specified in the **Operation** item above. For example, if an **Operation** of Add is selected above, entering the characters *8 in the **Constant** box will multiply the result of the Add operation by 8. The syntax of for this box should be <operator> <number>. Valid operators are + (addition),- (subtraction), * (multiplication), and / (division). Numbers may be integers or decimals.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set up to ten status thresholds criteria for each status condition per monitor instance. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the Formula Composite or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.

3 Enter a value applicable to the measurement parameter in the third text box.

4 To add another threshold setting, click the **New Error If** button and repeat the steps above.

5 Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the Formula Composite Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

35

FTP Monitor

The FTP Monitor attempts to log into an FTP server and retrieve a specified file. A successful file retrieval is an indication that your FTP server is functioning properly.

This chapter describes:	On page:
About the FTP Monitor	355
Configuring the FTP Monitor	357

About the FTP Monitor

If you provide FTP access to files, it is important to check that your FTP server is working properly. There is nothing more frustrating for a customer than to finally find the file they want, but then be unable to get it. The FTP monitor insures that you are the first to know if there is a problem.

To use this monitor you will need to:

- have network access to an FTP server
- know the relative paths, if any, to the files on the FTP server
- know an applicable username and password to access the files
- know the filenames of one or more files available for FTP transfer

In addition to retrieving specific files, the FTP Monitor can help you verify that the contents of files, either by matching the contents for a piece of text, or by checking to see if the contents of the file ever changes compared to a reserve copy of the file.

While you may have many files available for FTP from your site, it is not necessary to monitor every one. It is recommended that you check one small file and one large file.

A common strategy is to monitor a small file every 10 minutes or so just to verify that the server is functioning. Then schedule a separate monitor instance to FTP a large file once or twice a day. You can use this to test the ability to transfer a large file without negatively impacting your machine's performance. You can schedule additional monitors that watch files for content and size changes to run every 15 minutes to half hour. Choose an interval that makes you comfortable.

If you have very important files available, you may also want to monitor them occasionally to verify that their contents and size do not change. If the file does change, you can create a SiteScope alert that will run a script to automatically replace the changed file with a back-up file.

Status

The reading is the current value of the monitor. Possible values are:

- OK
- unknown host name
- unable to reach server
- unable to connect to server
- timed out reading
- content match error
- login failed
- file not found
- contents changed

The status is logged as either good or error. An error status is returned if the current value of the monitor is anything other than OK.

Configuring the FTP Monitor

The FTP Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the FTP Monitor.

Main Settings for the FTP Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the FTP server, how often this FTP Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this FTP monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the FTP Monitor should file transfer or download the FTP server. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

FTP Server

Enter the IP address or the name of the FTP server that you want to monitor. For example, you could enter either 206.168.191.22 or ftp.thiscompany.com.

File

Enter the file name to retrieve in this box, for example /pub/docs/mydoc.txt.

User Name

Enter the name used to log into the FTP server in this box. A common username for general FTP access is username anonymous.

Password

Enter the password used to log into the FTP server in this box. If using the anonymous login, the password is also anonymous.

Advanced Settings for the FTP Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the FTP Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Timeout

The number of seconds that the FTP monitor should wait for a file to complete downloading before timing-out. Once this time period passes, the FTP monitor will log an error and report an error status.

FTP Proxy

You may instruct SiteScope to run the FTP through a proxy server. Generally, if you use an FTP proxy you will have it set up in your browser. Enter that same information here. For example, proxy.thiscompany.com:8080. Remember to include the port.

Passive Mode

Check this box if you want SiteScope to use FTP passive mode. You use this mode to enable FTP to work through firewalls.

Match Content

Enter a string of text to check for in the returned file. If the text is not contained in the file, the monitor will display "no match on content". The search is case sensitive. You may also perform a regular expression match by enclosing the string in forward slashes, with an "i" after the trailing slash indicating case-insensitive matching. (For example, "/Size \d\d/" or "/size \d\d/i").

Check for Content Changes

Use this option to have SiteScope compare file contents to a previous, successful download of a file. The options for this setting are:

- **no content checking** - (default) SiteScope does not check for content changes
- **compare to last contents** - Any changed checksum will be recorded as the default after the change is detected initially. Thereafter, the monitor will return to a status of OK until the checksum changes again
- **compare to saved contents** - The checksum is a snapshot of a given page (retrieved either during the initial or a specific run of the monitor). If the contents change, the monitor will get a "content changed error" and will stay in error until the contents return to the original contents, or the snapshot is update by resetting the saved contents
- **reset saved contents** - Takes a new checksum of the file and saves the resulting checksum on the first monitor run after this option is chosen. After taking the updated checksum, the monitor will revert to "compare to saved contents" mode.

Unless this is set to "no content checking" (the default) SiteScope will record a checksum of the downloaded document the first time the monitor runs. The monitor then does a checksum comparison each subsequent time it runs. If the checksum changes, the monitor will report a status of "content changed error" and change state to error.

Generally, if you want to check for content changes in a file that normally is not expected to change, you will want to use the **compare to saved contents** option. This option saves a checksum "baseline" from the first successful download run of the monitor and compares all subsequent checksums to that baseline. The monitor will continue to report an error until 1) the subject file is replaced with the file having the original content (checksum) or 2) the **Check for Content Change** option is set to **reset saved contents** and the monitor is run with this setting. After running the monitor with this setting, the checksum baseline is updated and the monitor reverts back to the **compare to saved contents** option.

The **compare to last contents** option compares the checksum of the last successful download to that of the next successful download. If the checksums are different, an error is reported for that run of the monitor. The checksum from the most recent successful download then replaces the previous one. If the checksum of the next monitor run is the same as the new saved value, the monitor will change to a status of "good".

Proxy Server User Name

If the proxy server requires a name and password to access the file, enter the name here. Technical note: your proxy server must support Proxy-Authenticate for these options to function.

Proxy Server Password

If the proxy server requires a name and password to access the file, enter the password here. Technical note: your proxy server must support Proxy-Authenticate for these options to function.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set up to ten status thresholds criteria for each status condition per monitor instance. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the FTP or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the FTP Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- ➤ Do not report to Mercury Business Availability Center
- ➤ Report everything (all monitors and all measurements)
- ➤ Report monitor level data (no measurements)
- ➤ Report monitor level data and measurements with thresholds
- ➤ Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

36

IIS Server Monitor

The IIS Server Monitor allows you to monitor the availability and server statistics of an Microsoft IIS server on Windows NT systems. The error and warning thresholds for the monitor can be set on one or more IIS server performance statistics.

This chapter describes:	On page:
About the IIS Server Monitor	365
Configuring the IIS Server Monitor	366

About the IIS Server Monitor

Use the Microsoft IIS Server Monitor to monitor the server performance statistics from IIS servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate IIS Server monitor instance for each IIS server in your environment.

The IIS Server Monitor makes use of Performance Counters to measure application server performance. SiteScope will need to be running under an account that has the necessary administrative security privileges to access performance counter data from remote servers. If the servers you want to monitor are in a different domain, are governed under a different policy, or require a unique login different than the account SiteScope is running under, then you will need to define the connection to these servers under the NT Remote Preferences option in the SiteScope Preferences container.

The Remote Registry service must be running on the machine where the IIS server is running if IIS is running on Windows 2000.

The default run schedule for this monitor is every 10 minutes, but you can change it to run more or less often using the **Frequency** setting.

Configuring the IIS Server Monitor

The IIS Server Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the IIS Server Monitor.

Main Settings for the IIS Server Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the IIS Server, how often this IIS Server Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this IIS Server monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the IIS Server Monitor should system check the IIS Server. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Server

Choose the server where the IIS Server you want to monitor is running. Use the drop-down list to select a server from the list of remote servers that are available to the SiteScope agent.

Counters

You use the features associated with the **Counters** setting to choose and manage the metrics you want to monitor with the IIS Server Monitor. Use the following steps to select and add counters.

To select or add counters:

1. Click **Get Counters** to query the remote system. After SiteScope has successfully connected to the remote system, the Get Counters selection dialogue opens.
2. Use the features in the Get Counters selection dialogue screen to select the IIS Server metrics you want to monitor. Use the expandable menu controls as applicable to browse the available counters.
3. Use the check boxes to select between one and ten counters to be monitored.
4. Click **OK** to add the selected counters to the monitor configuration. The Get Counters selection dialogue closes and the monitor properties are updated with your selection.

Use the following steps to remove a counter from the selected counters list.

To remove or edit counters:

1. Click to edit the monitor for which you want to remove counters. Alternately, you may select the monitor you want to edit and click the Properties tab and click the **Edit** button. The monitor Properties screen opens.
2. Click the **Get Counters** button to open the Get Counters selection dialogue.
3. Clear the check box to the left of the current counter you want to remove.

   At this point, you may add other counters to the monitor by clicking the applicable check boxes.
4. Click **OK** at the bottom of the screen to update the monitor.

The performance parameters or counters available for the IIS Server Monitor include:

- Bytes Sent/sec
- Bytes Received/sec

- Get Requests/sec
- Post Requests/sec
- Maximum Connections
- Current Connections
- Current NonAnonymous Users
- Not Found Errors/sec
- Private Bytes (Process object)

Advanced Settings for the IIS Server Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the IIS Server Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set one or more status thresholds criteria for each status condition per monitor instance. The status of the monitor and any associated alert action will be set based on comparison of all the threshold criteria you define for the monitor. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the IIS Server or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the IIS Server Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

37

iPlanet Server Monitor

The iPlanet Server Monitor allows you to monitor the availability of SunONE/iPlanet and Netscape servers. The error and warning thresholds for the monitor can be set on one or more Netscape server performance statistics or HTTP response codes.

This chapter describes:	On page:
About the iPlanet Server Monitor	373
Configuring the iPlanet Server Monitor	375

Note: The SiteScope iPlanet Server Monitor is formerly known as the Netscape Server Monitor. Several file, name, and performance counter changes have been made to reflect the changes in the server product name and capabilities of the monitor.

About the iPlanet Server Monitor

Use the iPlanet Server Monitor to monitor the content of server administration pages for iPlanet and Netscape servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate monitor instance for each server you are running.

The following are requirements for using the iPlanet Server Monitor:

To monitor Current Activity statistics for iPlanet 4.1 servers:

1. You will need to know the username and password to access the iPlanet administrative server page. The URL for the main administrative page normally has the form of:
   http://*serveraddress:adminport*/https-admserv/bin/index
2. Identify the virtual server instance name you want to monitor. This should be available in the drop-down box to the right of the **Manage** button. Enter it in the place of *virtualserveraddressname* in the URL (see below).
3. Set up monitor using iPlanet 4.1 current activity counters using the URL of the following form:
   http://*serveraddress:adminport*/https-*virtualserveraddressname*/bin/sitemon?doit:

To monitor performance dump statistics for iPlanet 4.1 servers:

1. Modify the obj.conf file for each virtual server instance you want to monitor adding the line to enable perf dump. The conf entry normally has the form of:

   <Object ppath="path/Netscape/Server4/docs/.perf">
   Service fn=service-dump
   </Object>
2. Restart the server(s).
3. Access the performance dump page using the URL of the form:
   http://*serveraddress*:*http_port*/.perf
4. Set up the iPlanet Server Monitor using iPlanet 4.1 performance dump counters (see below).

To monitor server statistics for iPlanet 6.0 servers using HTTP:

1. You will need to know the username and password to access the iPlanet administrative server page. The URL for the main administrative page normally has the form of:
   http://serveraddress:adminport/https-admserv/bin/index
2. Identify the specific server instance names as shown in the drop-down box next to the **Manage** button. The server instance names are used as the virtualserveraddressname the URL for monitoring that server instance. The

URL needed to monitor the server statistics normally has the form of;
http://serveraddress:adminport/https-virtualserveraddressname/bin/instance-app/*pageStats*.jsp?pollInterval=15&vsname=All
where *pageStats* is replaced with a specific statistics page name as outlined below.

Note: For the value for vsname (virtual server name) you can replace All with a specific virtualserveraddressname to monitor specific server instances. For example:
http://serveraddress:adminport/https-virtualserveraddressname/bin/instance-app/*pageStats*.jsp?pollInterval=15&vsname=virtualserveraddressname

To monitor virtual server activity statistics substitute virtualServerStats for *pageStats*.
To monitor server connection status statistics substitute connectionStats for *pageStats*.
To monitor server DNS statistics for iPlanet 6.0 servers substitute dnsStats for *pageStats*.
To monitor Keep-Alive statistics substitute keepAliveStats for *pageStats*.

About Scheduling this Monitor

Depending on the activity on the server, the time to build the server monitor statistics Web page may take more than 15 seconds. You should test the monitor with an Update value of several minutes to allow the server to build and serve the server monitor statistics Web page before the SiteScope monitor is scheduled to run again.

Configuring the iPlanet Server Monitor

The iPlanet Server Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the iPlanet Server Monitor.

Main Settings for the iPlanet Server Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the iPlanet Web server, how often this iPlanet Server Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this iPlanet Server monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the iPlanet Server Monitor should system performance check the iPlanet Web server. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Counters

Choose the server performance parameters or counters you want to check with this monitor. The list to the right of this item displays those currently selected for this monitor. Use the **Get Counters** link to bring up the counters selection screen. Check or clear the check boxes on the Get Counters screen to select one or more counters to monitor on this server.

Note: Select only those counters that are applicable to the server version you want to monitor.

Do not edit the order of the counters in the selected counter text box. The counters must be maintained in the order they appear in the **choose counter** selection page.

The SunONE/iPlanet 4.1 performance parameters or counters available for the iPlanet Server Monitor include:

For Current Server Activity

- Bytes transferred
- Bad requests
- 200 - number of successful transactions processed by the server since the last server restart.
- 2xx - The number of the server handles status codes in the 200 to 299 range since the last server restart.
- 302 - The number of requests with a status of "found".
- 304 - The number of requests with a status of "not modified" in response to conditional GET requests.
- 3xx - The number of server handles status codes in the 300 to 399 range since the last server restart.
- 401 - The number of unauthorized requests handled by the server since the last server restart.
- 403 - The number of forbidden requests handled by the server since the last server restart.
- 4xx - The number of server handles status codes in the 400 to 499 range since the last server restart. This includes code 404 which is a status of "not found"
- 5xx - The number of server handles status codes in the 500 to 599 range since the last server restart. This includes code 500 which indicates a server internal error.
- xxx - all three digit HTTP response codes

For Server Performance Dump:Address

- ActiveThreads
- WaitingThreads
- BusyThreads
- Thread limits

- Total Sessions
- KeepAliveCount
- KeepAliveHits
- KeepAliveFlushes
- KeepAliveTimeout
- enabled - Indicated the state of the Cache feature
- CacheEntries
- Hit Ratio
- pollInterval
- NativePool:
- Idle/Peak/Limit - Returns numbers expressed in the format of nn/nn/nn
- Work queue length/Peak/Limit - Returns numbers expressed in the format of nn/nn/nn

The iPlanet 6.0 server performance parameters or counters available for the iPlanet Server Monitor include:

For Virtual Server statistics (virtualServerStats.jsp):

- Total Number Of Requests
- Number Of Bytes Received
- Number Of Bytes Sent
- Number Of Virtual Servers
- 200 - number of successful transactions processed by the server since the last server restart.
- 2xx - The number of the server handles status codes in the 200 to 299 range since the last server restart.
- 302 - The number of requests with a status of "found".
- 304 - The number of requests with a status of "not modified" in response to conditional GET requests.

- 3xx - The number of server handles status codes in the 300 to 399 range since the last server restart.
- 401 - The number of unauthorized requests handled by the server since the last server restart.
- 403 - The number of forbidden requests handled by the server since the last server restart.
- 404 - The number of page not found requests handled by the server since the last server restart.
- 4xx - The number of server handles status codes in the 400 to 499 range since the last server restart. This includes code 404 which is a status of "not found"
- 5xx - The number of server handles status codes in the 500 to 599 range since the last server restart. This includes code 500 which indicates a server internal error.
- Other - all three digit HTTP response codes

For Keep-Alive statistics (keepAliveStats.jsp):

- Maximum Keep-Alive Connections
- Keep-Alive Timeout
- Number Of Processes
- Keep-Alive Hits
- Keep-Alive Flushes
- Keep-Alive Refusals
- Keep-Alive Timeouts

For server DNS statistics (dnsStats.jsp):

- Maximum DNS Cache Entries
- Number Of Processes
- DNS Cache Hits
- DNS Cache Misses

For Cache statistics (cacheStats.jsp):

- Maximum Cache Age \(seconds\)
- Maximum Heap Cache Size
- Maximum Memory Cache Map Size
- Number Of Processes
- Cache Hits
- Cache Misses
- Info Cache Hits
- Info Cache Misses
- Content Cache Hits
- Content Cache Misses

For Connection statistics (connectionStats.jsp):

- Total Number Of Connections
- Maximum Number Of Queued Connections
- Peak Number Of Queued Connections
- Current Number Of Queued Connections
- Number Of Processes

URL

Select the URL you want to verify with this monitor. This URL should be the URL to the applicable server monitor statistics Web page for the server version you want to monitor. For iPlanet 4.1 servers this usually has the form of http://*servername:adminport*/https-*serveraddress*/bin/sitemon?doit. For iPlanet 6.0 servers, the URL of the monitor statistics Web page has the form http://*servername:adminport*/https-*instanceserveraddress*/bin/instance-app/ *page*Stats.jsp?pollInterval=15&vsname=All where *page*Stats.jsp is replaced with the file reference for the specific statistics page you want to monitor (see the list of counters above).

Note: The *servername:port* and *serveraddress* are not necessarily identical depending on if you access the administrator server pages locally or remotely. The SiteScope iPlanet Server Monitor generally needs to be configured using the full *serveraddress* and not the https-admserv syntax. Normally you can find the *serveraddress* in the **Select a Server** box on the main administration Web page.

Note: (Recommended for Advanced Users Only) The iPlanet Server Monitor can be used to monitor other server products in the SunONE product line that make their performance statistics available via an server monitor statistics Web page. In order to monitor other products you will need to know the URL of the access log or administration Web page for that product version. You will need to modify the regular expression in the _netscapeRegExp= entry of the SiteScope **master.config** file and add any additional counter strings to the **SiteScope/templates.applications/counters.iplanet** file to extract the applicable values from the administration logs.

Advanced Settings for the iPlanet Server Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the iPlanet Server Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Timeout

The number of seconds that the monitor should wait for a response from the server before timing-out. Once this time period passes, the monitor will log an error and report an error status.

Note: Depending on the activity on the server, the time to build the server monitor statistics Web page may take more than 15 seconds. You should test the monitor with an Timeout value of more than 60 seconds to allow the server to build and serve the server monitor statistics Web page before the SiteScope monitor is scheduled to run again.

HTTP Proxy

Optionally, a proxy server can be used to access the server. Enter the domain name and port of an HTTP Proxy Server.

Authorization User Name

If the server you want to monitor requires a name and password for access, enter the name in this box.

Authorization Password

If the server you want to monitor requires a name and password for access, enter the password in this box.

NT Challenge Response

Check this box if you want SiteScope to use Window's NT Challenge Response authorization when accessing the server.

Proxy Server User Name

If the proxy server requires a name and password to access the server, enter the name here. Technical note: your proxy server must support Proxy-Authenticate for these options to function.

Proxy Server Password

If the proxy server requires a name and password to access the server, enter the password here. Technical note: your proxy server must support Proxy-Authenticate for these options to function.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule

➤ Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set one or more status thresholds criteria for each status condition per monitor instance. The status of the monitor and any associated alert action will be set based on comparison of all the threshold criteria you define for the monitor. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the iPlanet Server or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the iPlanet Server Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

38

IPMI Monitor

You use the SiteScope IPMI Monitor to monitor component health and operation statistics for Intelligent Platform Management Interface enabled devices.

This chapter describes:	On page:
About the IPMI Monitor	387
System Requirements	387
Configuring the IPMI Monitor	388

About the IPMI Monitor

The Intelligent Platform Management Interface (IPMI) provides an interface for reporting on device operations such as whether fans are turning and voltage flowing within server hardware. This is becoming an important part of IT system management. You use the IPMI Monitor to monitor server and network element platforms to get a more complete view of component health in business critical IT infrastructures.

You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch key operational factors that can seriously impact availability and degrade performance. Create a separate monitor instance for each server you are running.

System Requirements

The following are requirements for using the IPMI Monitor:

- The device you want to monitor has to be IPMI-enabled. In most cases, this means that the device must be designed for IPMI sensing and include an separate, dedicated IPMI network adapter.
- You need to know the IP address of the IPMI network adapter for the device you want to monitor. In many cases, this IP address will be different than the IP address used for other network communication to and from the device. Use an applicable IPMI utility to query for the IP address or contact the applicable system administrator.

Configuring the IPMI Monitor

The IPMI Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the IPMI Monitor.

Main Settings for the IPMI Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the iPlanet Web server, how often this IPMI Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this IPMI monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the IPMI Monitor should system performance check the iPlanet Web server. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Server Name

Enter the IPMI server name or IP address of the IPMI network adapter.

Note: The IP address is normally not the same as the as the ordinary ethernet NIC adapter address.

Port Name

Enter the port number of the IPMI device. The default port number is 623.

User

Enter the user name required to connect the IPMI device

Password

Enter the password required to connect the IPMI device

Complete the items as described to establish a connection to the target server. When the necessary connection information is entered, click the **Get Counters** button to query the server for available metrics.

Counters

You use the features associated with the **Counters** setting to choose and manage the metrics you want to monitor with the IPMI Monitor. Use the following steps to select and add counters.

To select or add counters:

1. Click **Get Counters** to query the remote system. After SiteScope has successfully connected to the remote system, the Get Counters selection dialogue opens.
2. Use the features in the Get Counters selection dialogue screen to select the iPlanet Web server metrics you want to monitor. Use the expandable menu controls as applicable to browse the available counters.
3. Use the check boxes to select between one and ten counters to be monitored.

4 Click **OK** to add the selected counters to the monitor configuration. The Get Counters selection dialogue closes and the monitor properties are updated with your selection.

Use the following steps to remove a counter from the selected counters list.

To remove or edit counters:

1 Click to edit the monitor for which you want to remove counters. Alternately, you may select the monitor you want to edit and click the Properties tab and click the **Edit** button. The monitor Properties screen opens.

2 Click the **Get Counters** button to open the Get Counters selection dialogue.

3 Clear the check box to the left of the current counter you want to remove.

At this point, you may add other counters to the monitor by clicking the applicable check boxes.

4 Click **OK** at the bottom of the screen to update the monitor.

Advanced Settings for the IPMI Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the IPMI Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set one or more status thresholds criteria for each status condition per monitor instance. The status of the monitor and any associated alert action will be set based on comparison of all the threshold criteria you define for the monitor. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the IPMI or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the IPMI Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

39

JMX Monitor

The SiteScope JMX Monitor allows you to monitor the performance statistics of those Java-based applications that provide access to their statistics via the standard JMX remoting technology.

This chapter describes:	On page:
About the JMX Monitor	395
Usage Guidelines	396
Configuring the JMX Monitor	397

About the JMX Monitor

Standard JMX remoting technology is defined by JSR 160. This standard is already supported by several software vendors and is quickly gaining acceptance.

Here are some applications that currently support JSR 160 and information about how to monitor them:

- BEA WebLogic 9.x - Supports JSR 160, which can be enabled by following instructions found on the BEA Web site (http://www.e-docs.bea.com/wls/docs90/ConsoleHelp/taskhelp/channels/EnableAndConfigureIIOP.html).

  Once enabled, the JMX URL for monitoring the server follows the following form:

  service:jmx:rmi:///jndi/iiop://localhost:7001/weblogic.management.mbeanservers.runtime (The localhost is the server name or IP address that is running your WebLogic application.)

➤ Tomcat 5.x - Supports JSR 160, by defining the following properties to the JVM upon startup:

Dcom.sun.management.jmxremote

Dcom.sun.management.jmxremote.port=9999

Dcom.sun.management.jmxremote.ssl=false

Dcom.sun.management.jmxremote.authenticate=false

The above specifies the port as 9999. This value can be changed to any available port. Also, it specifies no authentication. If authentication is necessary, see the Java Sun Web site for more details (http://java.sun.com/j2se/1.5.0/docs/guide/jmx/tutorial/security.html). If the above properties are defined when starting Tomcat 5.x (on localhost), the following would be the JMX URL for monitoring it:

service:jmx:rmi:///jndi/rmi://localhost:9999/jmxrmi

Note: SiteScope 8.x runs within Tomcat 5.x, and thus can be monitored as described above.

➤ Many other vendors have recently released, or will soon release, versions of their software that are JSR 160 compliant, including JBoss, Oracle 10g, and IBM WebSphere.

You can find more information about JSR 160 on the Java Community Process Web site (http://www.jcp.org/en/jsr/detail?id=160).

Usage Guidelines

Use the JMX Monitor to monitor JMX statistics of a JSR 160 compliant application. You can monitor multiple parameters or counters with a single monitor instance. The counters available vary from application to application, but normally include both basic JVM performance counters as well as counters specific to the application. You may create one JMX Monitor instance for each application you are monitoring, or several monitors for the same application that analyze different counters.

The default run schedule for this monitor is every 10 minutes, but you can modify the monitor to run more or less often using the **Update every** setting.

Configuring the JMX Monitor

The JMX Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the JMX Monitor.

Main Settings for the JMX Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the LDAP database, how often this JMX Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this JMX monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the JMX Monitor should LDAP authentication request the LDAP database. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

JMX URL

The URL to gather JMX statistics. Typically the URL begins with service:jmx:rmi:///jndi, followed by information specific to the application. For examples of URLs used for WebLogic and Tomcat, see "About the JMX Monitor" on page 395.

Domain Filter

Domain filter to show only those counters existing within a specific domain (optional).

User Name

Username for connection to the JMX application (optional).

Password

Password for connection to the JMX application (optional).

Counters

Select the counters to monitor. Click **Get Counters** to change the selected counters.

Advanced Settings for the JMX Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the JMX Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set up to ten status thresholds criteria for each status condition per monitor instance. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the JMX or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the JMX Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- ➤ Do not report to Mercury Business Availability Center
- ➤ Report everything (all monitors and all measurements)
- ➤ Report monitor level data (no measurements)
- ➤ Report monitor level data and measurements with thresholds
- ➤ Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

40

LDAP Monitor

The LDAP Monitor verifies that a Lightweight Directory Access Protocol (LDAP) server is working correctly by connecting to it and performing a "simple" authentication. Optionally, it can check the result for expected content.

This chapter describes:	On page:
About the LDAP Monitor	403
Configuring the LDAP Monitor	404

About the LDAP Monitor

If your LDAP server is not working properly, the user will not be able to access and update information in the directory. Most importantly, the user will not be able to perform any authentication using the LDAP server. The other reason to monitor the LDAP server is so you can find performance bottlenecks -- if your End User and LDAP times are both increasing at about the same amount, the LDAP server is probably the bottleneck. If not, the bottleneck is probably somewhere else.

What to Monitor

The most important thing to monitor is the authentication of a specific user on the LDAP server. If more than one LDAP server is used, you will want to monitor each of the servers.

You may also choose to monitor round trip time of the authentication process.

About Scheduling this Monitor

You may want to monitor your most critical and most common queries as frequently as every 10-15 minutes.

Status

Each time the LDAP Monitor runs, it returns a status based upon the time it takes to perform the connection.

The status is logged as either OK, warning, or error. An error status or warning status is returned if the current value of the monitor is anything other than OK. Errors occur if SiteScope is unable to connect, receives an unknown hostname error, or the IP address does not match the hostname.

Configuring the LDAP Monitor

The LDAP Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the LDAP Monitor.

Main Settings for the LDAP Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the LDAP database, how often this LDAP Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this LDAP monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the LDAP Monitor should LDAP authentication request the LDAP database. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

LDAP Service Provider

Enter the constant that holds the name of the environment property for specifying configuration information for the service provider to use. The value of the property should contain a URL string (for example, "ldap://somehost:389"). This property may be specified in the environment, an applet parameter, a system property, or a resource file. If it is not specified in any of these sources, the default configuration is determined by the service provider.

LDAP Security Principal

Enter the constant that holds the name of the environment property for specifying the identity of the principal for authenticating the caller to the service. The format of the principal depends on the authentication scheme. If this property is unspecified, the behavior is determined by the service provider. This should be of the form (uid=testuser,ou=TEST,o=mydomain.com)

LDAP Security Credential

Enter the constant that holds the name of the environment property for specifying the credentials of the principal for authenticating the caller to the service. The value of the property depends on the authentication scheme. For example, it could be a hashed password, clear-text password, key, certificate, and so on. If this property is unspecified, the behavior is determined by the service provider.

Advanced Settings for the LDAP Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the LDAP Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Content Match

Enter a string of text to check for in the query result. If the text is not contained in the result, the monitor will display no match on content. The search is case sensitive. This works for XML tags as well. You may also perform a regular expression match by enclosing the string in forward slashes, with an i after the trailing slash indicating case-insensitive matching. (for example, /href=Doc\d+\.html/ or /href=doc\d+\.html/i). If you want a particular piece of text to be saved and displayed as part of the status, use parentheses in a Perl regular expression. For example /Temperature: (\d+). This would return the temperature as it appears on the page and this could be used when setting an Error if or Warning if threshold.

Object Query

Use this box to enter an object query to look at a LDAP object other than the default user **dn** object. For example, enter the mail object to check for an e-mail address associated with the dn object entered above. You must enter a valid object query in this text box if you are using a LDAP filter (see the description below).

LDAP Filter

Enter an LDAP filter in this text box in order to perform a search using a filter criteria. The LDAP filter syntax is a logical expression in prefix notation meaning that logical operator appears before its arguments. For example, the item sn=Freddie means that the **sn** attribute must exist with the attribute value equal to Freddie. Multiple items can be included in the filter string by enclosing them in parentheses, such as (sn=Freddie) and combined using logical operators such as the & (the conjunction operator) to create logical expressions. For example the filter syntax (& (sn=Freddie) (mail=*)) requests LDAP entries that have both a sn attribute of Freddie and a mail attribute. More information about LDAP filter syntax can be found at http://www.ietf.org/rfc/rfc2254.txt and also at http://java.sun.com/products/jndi/tutorial/basics/directory/filter.html

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set up to ten status thresholds criteria for each status condition per monitor instance. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the LDAP or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.

3 Enter a value applicable to the measurement parameter in the third text box.

4 To add another threshold setting, click the **New Error If** button and repeat the steps above.

5 Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the LDAP Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

41

Link Check Monitor

The Link Check Monitor checks the internal and external links on a Web page to insure that they can be reached. SiteScope begins checking links from a URL that you specify, verifies that linked graphics can be found, and follows HREF links to the referenced URLs. The monitor can be configured to check all of the links on your site or limited to a specified number of "hops" from the initial URL.

This chapter describes:	On page:
About the Link Check Monitor	413
Configuring the Link Check Monitor	414

About the Link Check Monitor

There is nothing more frustrating for your Web site visitors than trying to follow a broken link. Ensuring that your site is free of broken links is something that everyone knows they should do, but it is often the thing that gets moved to the bottom of the to-do list. This monitor can be set to check every link on your site, internal and external, every day, letting you know immediately which links have a problem.

Each time the Link Check Monitor runs, it returns a status and writes it in the monitoring log file. It also writes the total number of broken links, the total number of links, the total number of graphics, and the average time for retrieving a page.

What to Monitor

In addition to checking the links, a Link Report is created. This report can be viewed by choosing the **Summary** link in the **More** column. The report displays all the links checked, the status of each link, size, estimated download time via a 28.8 connection, and the page containing the link. You may reorder the entries in this table by clicking on the column heading that you want the entries to be sorted by. For example, if you want the entries to be sorted by retrieval time, click the **Time** column heading.

You should monitor the Web site for the availability of key content. This includes checking that image files and linked HTML files are accessible as referenced within the Web pages. Starting with your home page, the Link Check Monitor will branch out and check every link available on your entire site by default. If you only want it to check a portion of your site, specify the URL that links into the targeted area. You can limit the number of linked "hops" the monitor will follow in the Advanced Settings section. Even if you are not the person responsible for Web content, you can set the monitor to run once a day and have the alerts e-mailed directly to your Web content developer.

About Scheduling this Monitor

You probably only need to run the link monitor once a day to check for external links that have been moved or no longer work and internal links that have been changed. You can also run it on demand any time you do a major update of your Web site.

Configuring the Link Check Monitor

The Link Check Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the Link Check Monitor.

Main Settings for the Link Check Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the Web pages, how often this Link Check Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this Link Check monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the Link Check Monitor should hyperlink check the Web pages. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

URL

Enter the URL that will be the starting point for checking links (for example, http://demo.thiscompany.com). The link monitor will retrieve the page for this URL. Next, it will read the URLs for any links on the page. It will continue until it has checked all of the links on the site. Links to other servers will be checked but it will not continue and check all the links of those other servers.

Search External Links

Select this option to have the Link Check Monitor follow all links on each page and not just links that contain the original base URL.

Warning: Using this option may greatly increase the number of links that are tested and the amount of time required for the monitor to run. In some cases this may cause the monitor to run for more than 24 hours without being able to complete all of the link checks. If you select this option, be sure to limit the total number of links to test using the **Maximum Links** setting and limit the depth of the search using the **Maximum Hops** setting in the Advanced Settings.

Advanced Settings for the Link Check Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Link Check Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Pause

The delay, in milliseconds, between each link check. Larger numbers will lengthen the total time to check links but will decrease the load on the server.

Maximum Links

The maximum number of links this monitors will check. When the maximum number of links is reached the monitor will stop and report the results of those links that were checked. Increase this number if you have a large site and want to check every link on the site.

Maximum Hops

The maximum number of internal links that SiteScope should follow from the starting URL. For example, if you set the number of hops to three, SiteScope will check all internal pages that can be reached within 3 clicks from the starting URL. Limiting this number will reduce the number of URLs that SiteScope will follow or "hop" to, shortening the time to complete the report. SiteScope will not follow any links on external pages. Select one of the predefined choices using the drop-down menu. To enter your own limit, select Other from the drop-down menu and then enter a numeric value in the field below the menu.

Timeout

The number of seconds that the URL monitor should wait for a page to begin downloading before timing-out. Once this time period passes, the URL monitor will log an error and report an error status.

HTTP Proxy

Optionally, a proxy server can be used to access the URL. Enter the domain name and port of an HTTP Proxy Server.

Authorization User Name

If the URL specified requires a user name for access, enter the name in this box.

Authorization Password

If the URL specified requires a password for access, enter the password in this box.

Proxy Server User Name

If the proxy server requires a name to access the URL, enter the name here. Technical note: your proxy server must support Proxy-Authenticate for these options to function.

Proxy Server Password

If the proxy server requires a password to access the URL, enter the password here. Technical note: your proxy server must support Proxy-Authenticate for these options to function.

Post Data

Enter any form values required for the first page being checked. This is useful if you need to log in via an HTML form to reach the rest of the site that you are checking.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule

➤ Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set up to ten status thresholds criteria for each status condition per monitor instance. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the Link Check or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the Link Check Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

42

Log File Monitor

The Log File Monitor watches for specific entries added to a log file by looking for entries containing a text phrase or a regular expression.

This chapter describes:	On page:
About the Log File Monitor	423
Configuring the Log File Monitor	424

About the Log File Monitor

Each time the Log File Monitor runs, it examines only those log entries added since the last time it ran.

The "Run Alerts" setting control how alerts are triggered by this monitor. If "for each log entry matched" is chosen, then the monitor triggers alerts for every matching log entry found. In this way, the monitor acts much like an event forwarder. If "once, after all log entries have been checked" is chosen, then the monitor counts up the number of matches and triggers alerts based on the **Error if** and **Warning if** thresholds defined for the monitor.

What to Monitor

The Log File Monitor is useful for automatically scanning log files for error information. With SiteScope doing this for you at set intervals, you can eliminate the need to scan the logs manually. In addition, you can be notified of warning conditions that you might have otherwise been unaware of until something more serious happened. Each time that it runs this monitor, SiteScope starts from the point in the file where it stopped reading last time it ran. This insures that you are only notified of new entries and speeds the rate at which the monitor runs.

About Scheduling this Monitor

You can schedule your Log File Monitors to run as often as every 15 seconds. However, depending on the size of the log file, the total number of monitors you have running, and **Check from Beginning** option selected, the monitor may take 15 seconds or longer to check the file for the desired entries. The default update schedule is every 10 minutes which may be reasonable in most cases.

Configuring the Log File Monitor

The Log File Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the Log File Monitor.

Main Settings for the Log File Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the remote log file, how often this Log File Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this Log File monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the Log File Monitor should log file check the remote log file. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Server

If the log file is on a UNIX server, select the server name where the file located. Use the choose server link to access a list of remote UNIX servers that have been specified to SiteScope.

Note: Remote Windows computers will not appear in the Choose Server list. You use the UNC path to the remote log file to monitor log files in Windows networks.

Note: Monitoring log files using SSH on Windows platforms is not supported for this monitor.

Log File Pathname

Enter the pathname to the log file you want to monitor. For reading log files on remote UNIX machines, the path must be relative to the home directory of UNIX user account being used to login to the remote machine. For example, it may be necessary to provide the full path to the target file such as /opt/application/logs/user.log. You must also select the corresponding remote UNIX server in the Server field below. See the section "UNIX Remote Preferences" page for information on which UNIX user account is being used for the applicable remote server.

For reading log files on remote Windows NT/2000 servers, you use NetBIOS to specify the server and UNC path to the remote log file. For example, \\remoteserver\sharedfolder\filename.log

SiteScope will attempt to access the file using the permissions of the user SiteScope is using to run. If a direct connection via the operating system is unsuccessful, SiteScope will try to match the \\remoteserver with servers currently defined as remote NT connection profiles (displayed in the Remote NT Servers table). If an exact match is found for \\remoteserver in the remote NT connection profiles, SiteScope will try to use this connection profile to access the remote log file. If no matching server name is found, the monitor reports that the remote log file can not be found.

You can also monitor files local to the server where SiteScope is running. For example, C:\application\appLogs\access.log

Optionally, you can use special date and time regular expression variables to match on log file names that include date and time information. SiteScope compares the current system date and time data to find log files with corresponding date and time information. For example, you can use a syntax of

s/ex$shortYear$$0month$$0day$.log/

to match a current date-coded log file.

Check from Beginning

Select file checking option for this monitor instance. This setting controls what SiteScope will look for and how much of the target file will be checked each time that the monitor is run. The following table describes the options for this setting:

Checking Option	Description
Never	Check only newly added records, starting at the time that the monitor was created (not when the file was created). This is the default behavior.
First Time Only	Check the whole file once when the monitor is first created, then only for new records on each subsequent monitor run. Use this option to check a file that already had entries before the monitor was created or started.
Always	Always check the contents of the whole file. **Note:** Using this option may have undesired impact on SiteScope performance. Monitoring large log files with this option may use large amounts of memory and CPU time on the SiteScope server which can lead to other performance problems.

Run Alert

Select the method for running alerts for this monitor. If the **for each log entry matched** option is chosen, then the monitor triggers alerts for every matching entry found and the monitor will remain "good". If the **once, after all log entry have been checked** option is chosen, then the monitor counts up the number of matches and then triggers alerts based on the **Error If** and **Warning If** thresholds defined for the monitor.

Content Match

Enter the text to look for in the log entries. You can also use regular expression in this entry to match text patterns. Unlike the content match feature of other SiteScope monitors, the Log File Monitor content match is run repeatedly against the most recent content of target log file until all matches are found. This means the monitor not only reports if the match was found but also how many times the matched pattern was found. To match text that includes more than one line of text, add an s search modifier to the end of the regular expression.

Advanced Settings for the Log File Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Log File Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Rules File Pathname

Optional: In rare cases, it may be necessary to create a custom rules file to specify the log entries to match and the alerts to send. An example rules file is located in **<SiteScope install path>/SiteScope/Classes/CustomMonitor/test.rules**. Make a copy of this file and rename. There is no required naming convention. Open the file with the editor of your choice, and using the comments as a guideline, edit the file to meet your needs. When you are finished, type the full path name to your rules file in this box.

No Error on File Not Found

Check this box if you want this monitor to remain in GOOD status, if the file is not found.

Match Value Labels

Use this option to enter labels for the matched values found in the target log file. The match value labels are used as variables to access retained values from the **Content Match** expression for use with the monitor threshold settings. Separate multiple labels with a comma (,). The labels are used to represent any retained values from the **Content Match** regular expression in the parameters available for the status threshold settings (Error if, Warning if, and Good if). These labels are also displayed as the text labels in graphs generated for the retained values in management reports for this monitor.

Log File Encoding

If the log file content to be monitored uses an encoding that is different than the encoding used on server where SiteScope is running, enter the code page or encoding to use. Some examples of commonly used encodings are: Cp1252, Cp1251, Cp1256, Shift_JIS or EUC_JP. This may be necessary if the code page which SiteScope is using does not support the character sets used in the target log file. This will enable SiteScope to match and display the encoded log file content correctly.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set up to ten status thresholds criteria for each status condition per monitor instance. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the Log File or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the Log File Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

43

Mail Monitor

The Mail Monitor checks a Mail Server via the network. It verifies that the mail server is accepting requests, and also verifies that a message can be sent and retrieved. It does this by sending a standard mail message using SMTP and then retrieving that same message via a POP user account. Each message that SiteScope sends includes a unique key which it checks to insure that it does not retrieve the wrong message and return a false OK reading. If SiteScope is unable to complete the entire loop it generates an error message.

This chapter describes:	On page:
About the Mail Monitor	435
Configuring the Mail Monitor	436

About the Mail Monitor

Most companies are heavily dependent on e-mail today, and a missed or late e-mail message can spell disaster. The problem with e-mail is that unless you are expecting a message, you will not know it is missing. The Mail monitor checks to see that the mail server is both accepting and delivering messages.

What to Monitor

Most companies have both a primary and a secondary mail server. At companies that employ a firewall, there may even be a third, internal, mail server. Each of these servers should be monitored regularly.

Each time the Mail Monitor runs, it returns a status and writes it in the log file. It also writes the total time it takes to send and receive the mail message in the log file.

About Scheduling this Monitor

it is a good idea to monitor your primary mail server at least every five minutes. The other mail servers can be monitored less often. You may find it useful to set up a special mail account to receive the test e-mail messages send by SiteScope.

Configuring the Mail Monitor

The Mail Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the Mail Monitor.

Main Settings for the Mail Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the remote e-mail system, how often this Mail Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this Mail monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the Mail Monitor should e-mail transaction the remote e-mail system. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Action

Select the action the Mail Monitor should take with respect to the mail server. The Send & Receive option will allow you to send a test message to an smtp server and then receive it back from the POP3 or IMAP4 server to check that the mail server is up and running. Use the Receive Only option to check the incoming POP3 or IMAP4 mail servers for a message that was sent previously. This check is done by matching the content of the previously sent message. The Send Only option checks that the receiving mail server has accepted the message.

Note: If the **Receive Only** option is selected the Match Content text box must have a value to match against. Also note that if the **Receive Only** option is selected, you should use this monitor for a dedicated mail account that is NOT being accessed by any other mail client. If another mail client attempts to retrieve mail messages from the account that the Mail Monitor is monitoring in **Receive Only** mode, the monitor and the other mail client may lock each other out of the account such that neither is able to retrieve the messages.

Sending Mail Server (SMTP)

Enter the hostname of the SMTP mail server to which the test mail message should be sent (for example, mail.thiscompany.com).

Send To Address

Enter the mail address to which the test message should be sent. This should be the address for the POP account that you specified in the Mail Server User Name box. For example, if you specified "support" as the Mail Server User Name, the To Address might be "sysadmin@mycompany.com."

Receiving Protocol

Select the protocol used by the receiving mail server. You use the POP3 option to check the POP3 mail server for a sent message. You use the IMAP4 option to check the IMAP mail server for a sent message.

Receiving Mail Server

Enter the hostname of the POP3/IMAP4 mail server that should receive the test message. This can be the same mail server to which the test message was sent (for example, mail.thiscompany.com).

Receiving Mail Server User Name

Enter a POP user account name (for example, support) on the receiving mail server. A test e-mail message will be sent to this account and the Mail monitor will login to the account and verify that the message was received. No other mail in the account will be touched; therefore you can use your own personal mail account or another existing account for this purpose.

Note: If you use a mail reader that automatically retrieves and deletes messages from the server, there is a chance that the Mail Monitor will never see the mail message and will therefore report an error.

Receiving Mail Server Password

Enter a password, if necessary, for the receiving mail account.

Advanced Settings for the Mail Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Mail Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Receive Content Match

Enter a string of text to match against the contents of the incoming message. If the text is not contained in the incoming message, the monitor will be in error. This is for the receiving only option.(Example: Subject:MySubject). The search is case sensitive. Remember that HTML tags are part of a text document, so include the HTML tags if they are part of the text you are searching for (for example, "< B> Hello< /B> World"). This works for XML pages as well. You may also perform a regular expression match by enclosing the string in forward slashes, with an "i" after the trailing slash indicating case-insensitive matching. (For example, "/href=Doc\d+\.html/" or "/href=doc\d+\.html/i"). If you want a particular piece of text to be saved and displayed as part of the status, use parentheses in a regular expression. For example /Temperature: (\d+)/. This would return the temperature as it appears on the page and this could be used when setting an Error if or Warning if threshold.

Timeout

The number of seconds that the Mail monitor should wait for a mail message to be received before timing-out. Once this time period passes, the Mail monitor will log an error and report an error status.

POP Check Delay

After SiteScope sends the test message, it immediately logs into the mail account to verify that the message has been received. If the message has not been received, SiteScope will automatically wait 10 seconds before it checks again. You can adjust this wait time by indicating an alternate number of seconds to wait in this box.

Attachment

Enter the full path name of a file to add as an attachment to the e-mail message. Use this option to check that your e-mail server can accept and forward messages with attached files. Optionally, you can use a regular expression to insert date and time variables to create a filename or file path (for example: s/C:\firstdir\$shortYear$$0month$$0day$/)

Attachment Encoding

If the attachment file content uses an encoding that is different than the encoding used on server where SiteScope is running, enter the code page or encoding to use. Some examples of commonly used encodings are: Cp1252, Cp1251, Cp1256, Shift_JIS or EUC_JP. This may be necessary if the code page which SiteScope is using does not support the character sets used in the attachment file.

SMTP User

Enter the user name required for SMTP authentication if the SMTP server requires authentication before sending messages.

SMTP Password

Enter the password for the SMTP authentication (if required).

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set up to ten status thresholds criteria for each status condition per monitor instance. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the Mail or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.

3 Enter a value applicable to the measurement parameter in the third text box.

4 To add another threshold setting, click the **New Error If** button and repeat the steps above.

5 Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the Mail Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

44

MAPI Monitor

The SiteScope MAPI Monitor checks a Messaging Application Program Interface (MAPI) server to confirm that e-mail operations can be executed. The SiteScope MAPI Monitor is designed to test the operation of a Microsoft Exchange Server. The error and warning thresholds for the monitor are set based on the e-mail delivery time.

This chapter describes:	On page:
About the MAPI Monitor	445
System Requirements	445
Configuring the MAPI Monitor	449

About the MAPI Monitor

Use the MAPI Monitor to monitor the availability of Microsoft Exchange 5.5 and above. The monitor check for e-mail delivery time. This allows you to verify availability of the MAPI server by sending and receiving a test message in a Microsoft Exchange e-mail account. Create a separate MAPI monitor instance for each Microsoft Exchange server in your environment.

System Requirements

There are several important configuration requirements that must be performed or verified before the MAPI Monitor can be used. This section describes the steps you use to configure your environment for this monitor. The following are several definitions that are used in the steps listed below.

Local Administrator

An account that has administrative privileges on the local machine. An account can have this privilege either implicitly by having Domain Admin privileges or explicitly by adding as a member of the Administrators group on the local machine. Consult your system administrator, if necessary, for help with creating accounts.

MailBox Owner

This is an "owner" account for which an Exchange mailbox has been set up. In order to use the MAPI Monitor, this account must be a Local Administrator (see definition above) on the SiteScope server.

SiteScope User

This is the account that is used to run the SiteScope service. This account must also be a Local Administrator (see definition above).

The following setup steps must be performed before creating a MAPI Monitor:

To prepare the system for using the MAPI Monitor:

1 **Create mailbox accounts on each Exchange Server to be monitored with the MAPI monitor.**

Exchange mailbox accounts will be used by SiteScope to measure the roundtrip time for a message to originate and arrive in a mailbox account. The MAPI Monitor setup page supports up to two mailboxes per Exchange Server. If only one mailbox is specified on the MAPI Monitor setup page the same mailbox can be used for the sender and receiver accounts. Consult your Exchange system administrator if you need help setting up mailbox accounts for use with the SiteScope MAPI monitor.

2 **Add each Exchange Mailbox Owner to the Administrators users group on the SiteScope server.**

The Mailbox Owner accounts setup in step 1, which are by definition domain logons, must be added as to the Administrators group on the SiteScope server.

- Click **Start > Settings > Control Panel > Users and Passwords > Advanced tab** or open the Computer Management utility and expand

the **Local Users and Groups** folder in the left pane and click the **Groups** folder.

- Double-click the Administrators group icon to open the Administrators Properties window.
- Click the **Add** button to add each Mailbox Owner you expect to use with the MAPI Monitor.

Note: Make sure that the domain logon description is of the form domain\logon.

---

3 Install Microsoft Outlook or an equivalent MAPI 1.0 mail client on the SiteScope server.

The SiteScope server requires a MAPI 1.0 client such as Outlook XP or Outlook 2003 or later. Consult your system administrator, if necessary, for help installing a compliant MAPI client.

4 Configure Outlook for the MailBox User

After logging in to the SiteScope server as the MailBox User created in step 1 the Outlook wizard may start for setting up an Outlook profile for the mail box. If an Outlook client is already installed, then you may run that Outlook client and click **Tools > e-mail Accounts** to create a profile for the mailbox/logon you intend to use with the MAPI Monitor. See your Exchange System administrator for help configuring an Outlook client on your SiteScope server if necessary.

Creating an Outlook profile is not necessary, although it may be helpful for the purpose of troubleshooting. Once the wizard prompts you to set up a profile you can cancel to exit the wizard.

5 Verify that the SiteScope User logon is a member of Administrators group or a domain administrator account.

Important: The SiteScope User account must be a Local Administrator or be a member of the domain admins group.

To change the logon account for the SiteScope User:

- Open the **Services** control utility on the SiteScope server.
- Right-click the **SiteScope** service entry and click **Properties**. The SiteScope Properties settings screen opens.
- Click the Logon properties tab.
- Verify that the SiteScope User is run as a member of Administrators group or a domain logon account. To change the logon properties, click the **This account** radio button and enter the SiteScope User logon.
- Restart the SiteScope server after making changes to the SiteScope service logon account.

6 Add the SiteScope User account to the "Act as part of the operating system" local security policy.

To add the SiteScope User account to the "Act as part of the operating system" local security policy.

- Click **Start > Programs > Administrative Tools > Local Security Policy**. The Local Security Policy panel opens.
- Click the **Local Policies** folder in the left pane and then click the **User Rights Assignments** folder to display the list of policies.
- Double-click the "Act as part of the operating system" policy item in the right pane. The Local Security Policy Setting list opens.
- If the SiteScope User is not in the list of logons for this security policy setting then it must be added now. Click the Add button to bring up the Select Users or Groups window.
- Enter the SiteScope User logon using the domain\logon format if the SiteScope User is a domain account.
- After adding the SiteScope service logon you must reload the security settings. To do this, right-click the **Security Settings** root folder in the left pane and click **Reload**.
- Restart the SiteScope service after making changes to security policy.

The default run schedule for this monitor is every 10 minutes, but you can change it to run more or less often using the **Frequency** setting.

Configuring the MAPI Monitor

The MAPI Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the MAPI Monitor.

Main Settings for the MAPI Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the Exchange e-mail system, how often this MAPI Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this MAPI monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the MAPI Monitor should e-mail system check the Exchange e-mail system. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Server

Enter the hostname or address of a Microsoft Exchange Server. The name can be an IP address or other name that can be resolved by the DNS server. It is recommended that you copy the server name as it appears in the Properties of the e-mail account you will be using with this monitor.

Mailbox

Enter the name (alias) of the mailbox to be used for this monitor. This is often the e-mail account name but it may be a different name. It is recommended that you copy the mailbox name as it appears in the E-Mail Account properties for the e-mail account you will be using with this monitor.

Domain

Enter the domain to which both the owner of the mailbox being used and the Microsoft Exchange server belong.

Note: The owner of the mailbox to be used by this monitor must also have administrative account privileges on the machine where SiteScope is running. SiteScope also needs user account access to the domain where the Microsoft Exchange server is running.

User Name

Enter the NT account login name for the user associated with the above e-mail account.

User Password

Enter the NT account login password for the user name above.

Advanced Settings for the MAPI Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the MAPI Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Transaction timeout

Enter the number of seconds for the monitor to wait for the message to arrive before the monitor should timeout. The monitor will report an error if timeout value is met before the e-mail message is delivered.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule

➤ Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set one or more status thresholds criteria for each status condition per monitor instance. The status of the monitor and any associated alert action will be set based on comparison of all the threshold criteria you define for the monitor. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the MAPI or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the MAPI Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

45

Memory Monitor

The Memory Monitor provides a tool for you to track how much virtual memory is currently in use on a server. Running out of memory can cause server applications to fail and excessive paging can have a drastic effect on performance.

This chapter describes:	On page:
About the Memory Monitor	455
Configuring the Memory Monitor	457

About the Memory Monitor

What to Monitor

One of the primary factors that can affect your Web server's performance is memory. The two most important measurements to detect problems in this area are Pages per Second and Percentage of Virtual Memory Used, both monitored by the SiteScope Memory Monitor.

Each time the Memory Monitor runs, it returns a status message and writes it in the monitoring log file.

About Scheduling this Monitor

In most environments, the Memory Monitor does not put a heavy load on your server. For monitoring remote UNIX servers, SiteScope will usually need to open a telnet or SSH connection to the remote server. While the monitor actions generally do not load the either server, managing a large number of remote connections can results in some performance problems. You use the error and warning thresholds to have SiteScope notify you if memory on a remote server starts to get low.

Common Problems and Solutions

Pages per second measures the number of virtual memory pages that are moved between main memory and disk storage. If this number is consistently high (>10 pages/sec), system performance is being affected. One solution is to add more memory. Another solution is to turn off non-critical services that are using memory, or move these services to a different machine. The SiteScope Service Monitor measures the memory usage for each service.

Percentage of Virtual Memory Used measures the percentage of memory and paging file space used. If this number reaches 100%, services that are running may fail and new ones will not be able to start. Increasing the size of the paging file may solve the immediate problem but may decrease performance by increasing paging. A slow increase in Virtual Memory Used is often caused by a memory leak in a service. The SiteScope Process Detail tool (available when you click the tools link listed in the Monitor Detail Table) can be used to view the memory used by each service. The ideal solution is to install an upgraded version of the service without the leak. An interim solution is to use the SiteScope Service Monitor to measure the service size and invoke a SiteScope Script alert to restart the service when it becomes too large. If restarting the service does not fix the leak, it may be necessary to add a SiteScope Script alert to restart the server when memory usage is too high.

Configuring the Memory Monitor

The Memory Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the Memory Monitor.

Main Settings for the Memory Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the remote server, how often this Memory Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this Memory monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the Memory Monitor should memory usage check the remote server. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Server

Choose the server for which you want to monitor Memory. The default is to monitor memory on the server on which SiteScope is installed. Use the drop-down list to select a server from the list of remote servers that are available to the SiteScope agent.

Advanced Settings for the Memory Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Memory Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set up to ten status thresholds criteria for each status condition per monitor instance. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the Memory or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.

3 Enter a value applicable to the measurement parameter in the third text box.

4 To add another threshold setting, click the **New Error If** button and repeat the steps above.

5 Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the Memory Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

46

Network Bandwidth Monitor

You use the Network Bandwidth Monitor to monitor SNMP-enabled network appliances such as routers and switches. The error and warning thresholds for the monitor can be set on one or more different objects. This monitor type also provides a Real-time metrics report, available as a link in the More column on the Group Detail Page.

This chapter describes:	On page:
About the Network Bandwidth Monitor	463
Configuring the Network Bandwidth Monitor	464
Device Specific Metrics Config File: netbandwidth.xml	472

About the Network Bandwidth Monitor

The Network Bandwidth Monitor operates like many other browsable monitors: it gathers information from a source and allows the user to choose which items in the tree it should monitor. It works by connecting to the specified network component and returning a list of interfaces.

The MIB files in SiteScope/templates.mib are then used to create a browsable tree that contains names and descriptions of the objects found during the traversal. Note that an object may or may not be displayed with a textual name and description, depending on the MIB's available in SiteScope/templates.mib. SiteScope does not display objects for user selection when it has no knowledge of how to display those objects. For example, a plain OctetString may contain binary or ascii data, but SiteScope has no way to decode and display this data correctly without more information.

The default run schedule for this monitor is every 10 minutes, but you can change it to run more or less often using the Frequency setting.

Configuring the Network Bandwidth Monitor

The Network Bandwidth Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the Network Bandwidth Monitor.

Main Settings for the Network Bandwidth Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the network system, how often this Network Bandwidth Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this Network Bandwidth monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the Network Bandwidth Monitor should system check the network system. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Server

Enter the name of the server you want to monitor.

SNMP Version

Select the version of SNMP to use when connecting.

V1/V2 Community

Enter the community string (valid only for version 1 or 2 connections).

SNMP V3 Authentication Type

Select the type of authentication to use for version 3 connections.

SNMP V3 Username

Enter the username for version 3 connections.

SNMP V3 Authentication Password

Enter the authentication password to use for version 3 connections.

SNMP V3 Privacy Password

Enter the privacy password if DES privacy encryption is desired for version 3 connections. Leave blank if you do not want privacy.

SNMP V3 Context Engine ID

Enter a hexadecimal string representing the Context Engine ID to use for this connection. This is applicable for SNMP V3 only.

SNMP V3 Context Name

Enter the Context Name to use for this connection. This is applicable for SNMP V3 only.

Counters

You use the features associated with the **Counters** setting to choose and manage the metrics you want to monitor with the Network Bandwidth Monitor. Use the following steps to select and add counters.

To select or add counters:

1. Click **Get Counters** to query the remote system. After SiteScope has successfully connected to the remote system, the Get Counters selection dialogue opens.
2. Use the features in the Get Counters selection dialogue screen to select the network system metrics you want to monitor. Use the expandable menu controls as applicable to browse the available counters.

3 Use the check boxes to select between one and ten counters to be monitored.

4 Click **OK** to add the selected counters to the monitor configuration. The Get Counters selection dialogue closes and the monitor properties are updated with your selection.

Use the following steps to remove a counter from the selected counters list.

To remove or edit counters:

1 Click to edit the monitor for which you want to remove counters. Alternately, you may select the monitor you want to edit and click the Properties tab and click the **Edit** button. The monitor Properties screen opens.

2 Click the **Get Counters** button to open the Get Counters selection dialogue.

3 Clear the check box to the left of the current counter you want to remove.

At this point, you may add other counters to the monitor by clicking the applicable check boxes.

4 Click **OK** at the bottom of the screen to update the monitor.

Advanced Settings for the Network Bandwidth Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Network Bandwidth Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Device Type

Select an optional device type for device specific monitoring. The default is Do not monitor device-specific metrics. By specifying a device type, you will enable the Network Bandwidth monitor to watch certain device-specific metrics. See the section entitled Device Specific Metrics Config File for more information on controlling the metrics associated with these device types and on adding new device types.

Duplex or Half-Duplex

Select the duplex state to use when calculating percent bandwidth utilized for all selected interfaces on this device.

Interface Index

Metrics for network interfaces on an SNMP-enabled device are presented as a table of management information (the ifTable), where each row corresponds to a different interface. Unfortunately, there is no requirement that the mapping from interface-to-row in this table remain constant across device reboots. The Interface Index parameter may help prevent the interfaces SiteScope is monitoring from becoming confused after a device restarts.

The three possible options are:

- Indexed by Description The ifDescr field of the ifTable is used to maintain monitoring consistency across device reboots.
- Indexed by Physical Address The ifPhysAddr field of the ifTable is used to maintain monitoring consistency across device reboots.
- Indexed by ifTable Row Number SiteScope will assume that the interfaces remain in the same row in the ifTable across device reboots.

Note: Some devices (Cisco, for instance) may have a configuration option to not jumble the position of interfaces in the ifTable during reboot. This may be the safest option, as not all interfaces may always have a unique ifDescr, and not all interfaces may have an ifPhysAddr (loopback interfaces do not typically have a physical address).

Show Bytes In/Out

Select this option to display a graph for bytes in/out along with the percent bandwidth utilized on the Real-Time Metrics page.

Real-Time Data Time Window

Enter the number of hours for which real-time graph data should be stored.

Real-Time Data Vertical Axis

Enter the maximum value on the vertical axis for real-time graphs (leave blank to have this automatically calculated by SiteScope)

Timeout

Enter the total time, in seconds, that SiteScope should wait for all SNMP requests (including retries) to complete.

Retries

Enter the number of times each SNMP GET request should be retried before SiteScope considers the request to have failed.

Port

Enter the port to use when requesting data from the SNMP agent. The default of 161 is the port on which an SNMP agent will typically be listening.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set one or more status thresholds criteria for each status condition per monitor instance. The status of the monitor and any associated alert action will be set based on comparison of all the threshold criteria you define for the monitor. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the Network Bandwidth or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the Network Bandwidth Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

Device Specific Metrics Config File: netbandwidth.xml

The Network Bandwidth Monitor may be customized for use with specific devices which implement non-standard or vendor-specific OIDs. By editing the netbandwidth.xml file (found in the templates.applications directory), the user may add new Device Types which contain a set of OIDs to monitor.

Here is an example of a Device Type from the default netbandwidth.xml file:

```
<device>
        <identifier>cisco</identifier>
        <displayName>Cisco Routers and Switches</displayName>
        <deviceMetrics>
            <metric>
                <OID>1.3.6.1.4.1.9.9.109.1.1.1.1.7</OID>
                <metricName>CPU Usage</metricName>
                <units>percent used</units>
                <realTime>true</realTime>
                <sameGraph>true</sameGraph>
                <multipleInstances>all</multipleInstances>
            </metric>
            <metric>
                <OID>1.3.6.1.4.1.9.9.48.1.1.1.5</OID>
                <metricName>Memory</metricName>

<metricNameOID>1.3.6.1.4.1.9.9.48.1.1.1.2</metricNameOID>
                <units>bytes free </units>
                <realTime>true</realTime>
                <sameGraph>true</sameGraph>
                <multipleInstances>all</multipleInstances>
            </metric>
        </deviceMetrics>
    </device>
```

This entry specifies a new type of device entitled, "Cisco Routers and Switches". When this device type is selected in the Network Bandwidth Monitor, OID's for CPU and memory pool usage will be monitored. If multiple instances of this data are found on the device, they will all be recorded individually. In addition, they will both be reported on the real-time report graphs, and multiple instances of the same OID will be charted on the same real-time graph. For instance, a router with three memory pools (CPU, IO 1, and IO 2) will have a real-time report with a single graph for memory pool data, containing a total of three lines (one for each pool).

Below is a detailed description of the meaning of each XML tag in the config file. You may wish to consult this list when creating a new device type or when adding new metrics to existing device types.

The identifier Tag

This is for use by SiteScope to uniquely identify the device entry. For that reason, the value of this tag must be unique in the netbandwidth.xml file.

The displayName Tag

As its name suggests, this option controls the text that is displayed on the Network Bandwidth Monitor's Add/Edit page. You should choose a short, descriptive phrase that will help you to remember what type of device this entry is intended to monitor.

The deviceMetrics Tag

This tag encloses all of the metrics which should be monitored for this type of device.

The metric Tag

The metric tag encloses all of the properties associated with a single metric on the device.

The OID Tag

The OID tag contains the object identifier (OID) of the metric. This OID does not need to correspond to a single object instance. If multiple instances are found under the given OID, then all of them are retrieved. To use the Cisco memory pool example again, if the user wished to limit the metric to one memory pool, then the OID should contain the specific instance the user is interested in: <OID>1.3.6.1.4.1.9.9.48.1.1.1.5.1</OID> Otherwise, the user can specify the OID with no index to indicate that all memory pool instances should be retrieved: <OID>1.3.6.1.4.1.9.9.48.1.1.1.5</OID>

The metricName Tag

This tag specifies the base name to use for the retrieved instance(s). If no metricNameOID is specified, then this name will be used to create names for multiple instances of the metric.

The metricNameOID Tag

When present, this tag instructs the Network Bandwidth Monitor to ask the device for a name or series of names to use for the instance(s) retrieved for the given OID. This is particularly useful for columnar data, where one column in a MIB table contains data and a corresponding column contains descriptive names for the data. The value given in this tag must be a valid OID.

The units Tag

The units tag is, as the name suggests, used to give the units that should be displayed with the metric. This can be any text value, and has no impact on any calculations done on the data.

The realTime Tag

The value of this option must be either "true" or "false". When "true", this metric will appear on a graph in the "Real-Time Metrics" report page.

The sameGraph Tag

The value of this option must be either "true" or "false". It is only applicable to a metric for which multiple instances are present. The effect of setting this option to "true" is that all instances of the metric will appear in the same graph on the "Real-Time Metrics" report page.

The multipleInstances Tag

This tag specifies what the Network Bandwidth Monitor should do with OID's for which it retrieves more than one instance of data. Usually, the all option is the best selection, as it causes all instances to be displayed and graphed. The complete list of options includes:

- all causes all retrieved instances to be reported individually
- average causes all retrieved instances to be averaged
- min causes only the minimum of the retrieved instances to be reported
- max causes only the maximum of the retrieved instances to be reported

47

Network Monitor

The Network Monitor provides a tool you can use to track network statistics for server where SiteScope is running. Information provided by this monitor can help you track down performance problems related to the network interface on the SiteScope server.

This chapter describes:	On page:
About the Network Monitor	477
Configuring the Network Monitor	478

About the Network Monitor

What to Monitor

SiteScope performance is impacted by the network interface on the server where SiteScope is running. The actual number of bytes being passed in and out of your server as well as the number of packets in error are all critical measures of a server's performance and are tracked by the Network Monitor. In addition, active connections are tracked.

About Scheduling this Monitor

In most environments, scheduling the Network Monitor to run every 10 minutes should be sufficient. You use the error and warning thresholds to have SiteScope notify you if network traffic on the server gets too high.

Common Problems and Solutions

Packet Errors measure the number of packets that failed to reach the destination IP address. This can indicate a faulty network interface or media. If the problem shows up on several servers that are topologically close, it is likely the media. If this condition occurs on only one isolated server, you can suspect the interface.

Throughput indicators let you know how fully utilized your network interface is. For instance, if you are running on a conventional ethernet interface and you see numbers approaching 10 megabits / sec., the interface is nearly saturated.

Connections is the count of open ports on your network interface. This measure should settle at some predictable level. Continuous climbing of the connection count indicates an error condition or run-away condition that will eventually slow the server due to resource constraints.

Status

Each time the Network Monitor runs, it returns a reading and a status message and writes them in the SiteScope monitor logs.

The reading is the current value of the monitor, such as 40% saturated. The status is logged as either OK, warning, or error. A warning status is returned if the bytes out per second is more than 80% full. Full is defined as a fully saturated standard ethernet bandwidth or 10 megabits / sec. An error status is returned if bytes out per second is more than 90% saturation.

Configuring the Network Monitor

The Network Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the Network Monitor.

Main Settings for the Network Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the local network interface, how often this Network Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this Network monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the Network Monitor should network interface check the local network interface. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Advanced Settings for the Network Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Network Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set up to ten status thresholds criteria for each status condition per monitor instance. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the Network or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the Network Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

48

News Monitor

The News Monitor verifies that a news server can be connected to, and is responding. It also measures how long it takes to make a connection, and how many articles are currently in the specified news groups.

This chapter describes:	On page:
About the News Monitor	485
Configuring the News Monitor	486

About the News Monitor

Running the News Monitor on a regular basis can save you the headaches associated with the entire office coming in to tell you they can not read their news groups. With regular monitoring, you should be able to address problems before they impact the users.

In addition, you can manage the number of articles that are allowed to queue up, deleting them before they cause disk space problems.

About Scheduling this Monitor

Monitoring your news server every 10 minutes is normally sufficient. You can schedule the monitor to run more frequently if necessary.

Status

Each time the News Monitor runs, it returns a status message and writes it in the monitoring log file. It also writes the total time it takes to receive a response from the news server, and the number of articles available for each of the specified news groups.

The reading is the current value of the monitor. The possible values for the News Monitor are:

- OK
- unknown host name
- unable to reach server
- unable to connect to server
- timed out reading
- <news group> not found - the given news group was not found on the news server
- permission denied for connection - the connection could not be made, probably because the news server was configured to allow connections from a limited range of addresses.
- login expected - the news server expected a user name and password, but none were provided. In this case, enter a user name and password under the Advanced Settings section of the monitor.
- login failed, unauthorized - the user name and password were not accepted by the news server

The status is logged as either good or error. An error status is returned if the current value of the monitor is anything other than OK.

Configuring the News Monitor

The News Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the News Monitor.

Main Settings for the News Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the network news server, how often this News Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this News monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the News Monitor should news post check the network news server. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

News Server

Enter the IP address or the name of the news server that you want to monitor. For example, you could enter either 206.168.191.21 or news.thiscompany.com. If the port is not the standard news port, add the port after the server with a colon, for example, news.thiscompany.com:7777.

News Groups

Optionally enter a one or more news groups that will be checked, separated by commas. Each of these news groups will be checked for the current number of articles available in that news group - the reading of the monitor is the sum of articles available for each of the specified news groups.

Advanced Settings for the News Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the News Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Timeout

The number of seconds that the News monitor should wait for all of news transactions to complete before timing-out. Once this time period passes, the News monitor will log an error and report an error status.

User Name

If your News server requires authorization, enter a valid user name here.

Password

If your News server requires authorization, enter a valid password here.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set up to ten status thresholds criteria for each status condition per monitor instance. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the News or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the News Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

49

Oracle9i Application Server Monitor

The Oracle9i Application Server Monitor allows you to monitor the availability and performance statistics of a Oracle9i Application Server. The error and warning thresholds for the monitor can be set on one or more Oracle9i server performance statistics.

This chapter describes:	On page:
About the Oracle9i Application Server Monitor	493
Configuring the Oracle9i Application Server Monitor	494

About the Oracle9i Application Server Monitor

Use the Oracle9i Application Server Monitor to monitor the server performance data for Oracle9i servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate monitor instance for each Oracle9i Application server in your environment.

Note: You must enable Web caching on the Oracle 9i Application Server in order to use the Oracle9i Application Server Monitor.

The default run schedule for this monitor is every 10 minutes, but you can change it to run more or less often using the **Frequency** setting.

Configuring the Oracle9i Application Server Monitor

The Oracle9i Application Server Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the Oracle9i Application Server Monitor.

Main Settings for the Oracle9i Application Server Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the Oracle9i server, how often this Oracle9i Application Server Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this Oracle9i Application Server monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the Oracle9i Application Server Monitor should server system check the Oracle9i server. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

URL

Enter the server administration URL for the server you want to monitor. The URL will normally have the form of http://*server:port*/webcacheadmin?SCREEN_ID=CGA.Site.Stats&ACTION=Show.

Counters

Choose the server performance parameters or counters you want to check with this monitor. The table list to the right of this item displays those currently selected for this monitor. Click **Get Counters** to bring up the counters selection screen. Check or clear the check boxes on the Get Counters screen to select one or more counters to monitor on this server. The performance parameters or counters available for the Oracle9i Application Server Monitor include:

- Up/Down Time(up/down)
- Completed Requests(number/sec)
- Completed Requests(max/sec)
- Completed Requests(avg/sec)
- Completed Requests(total)
- Latency(avg this interval)
- Latency(avg since start)
- Load(now)
- Load(max)
- Active Sessions(now)
- Active Sessions(max)
- Apology Pages Served(Network Error - number this second)
- Apology Pages Served(Network Error - total)
- Apology Pages Served(Site Busy - number this second)
- Apology Pages Served(Site Busy - total)
- Application Web Server Backlog(now)
- Application Web Server Backlog(max)

Advanced Settings for the Oracle9i Application Server Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Oracle9i Application Server Monitor and its display in the product interface. See “Common Monitor Settings” in the chapter “Working with SiteScope Monitors” for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Timeout

The number of seconds that the monitor should wait for a response from the server before timing-out. Once this time period passes, the monitor will log an error and report an error status.

HTTP Proxy

Optionally, a proxy server can be used to access the server. Enter the domain name and port of an HTTP Proxy Server.

Authorization User Name

If the server you want to monitor requires a name and password for access, enter the name in this box.

Authorization Password

If the server you want to monitor requires a name and password for access, enter the password in this box.

NT Challenge Response

Check this box if you want SiteScope to use Window's NT Challenge Response authorization when accessing the server.

Proxy Server User Name

If the proxy server requires a name and password to access the server, enter the name here. Technical note: your proxy server must support Proxy-Authenticate for these options to function.

Proxy Server Password

If the proxy server requires a name and password to access the server, enter the password here. Technical note: your proxy server must support Proxy-Authenticate for these options to function.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set one or more status thresholds criteria for each status condition per monitor instance. The status of the monitor and any associated alert action will be set based on comparison of all the threshold criteria you define for the monitor. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the Oracle9i Application Server or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1 Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.

2 Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.

3 Enter a value applicable to the measurement parameter in the third text box.

4 To add another threshold setting, click the **New Error If** button and repeat the steps above.

5 Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the Oracle9i Application Server Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see “Common Monitor Settings” in the chapter Chapter 2, “Working with SiteScope Monitors.”

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see “Working with Categories” in *Working with Monitor Administration*.

50

Oracle Database Monitor

The Oracle Database Monitor allows you to monitor the availability of an Oracle database server (versions 8i and 9i plus some earlier versions). The error and warning thresholds for the monitor can be set on one or more Oracle server performance statistics.

This chapter describes:	On page:
About the Oracle Database Monitor	503
Configuring the Oracle Database Monitor	505

About the Oracle Database Monitor

Use the Oracle Database Monitor to monitor the server performance statistics from Oracle Database servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate Oracle Database Monitor instance for each Oracle database server in your environment.

The following are several key requirements for using the Oracle Database Monitor:

- You must have a copy of the applicable Oracle JDBC database driver file (for example, classes12.zip) on the SiteScope server. Copy the downloaded driver file into the **<SiteScope install path>\SiteScope\java\lib\ext** subdirectory. DO NOT unzip the file. Stop and restart the SiteScope service after copying the driver file to the SiteScope machine.

Note: More than one driver file is available for download. Some drivers support more than one version of Oracle database (for example, the classes12.zip Oracle JDBC thin driver) while others only support a particular version. If you are monitoring a recent version of Oracle database, you should download the latest version of the database driver.

- You must supply the correct **Database Connection URL**, a database username and password when setting up the monitor. The syntax of the Database Connection URL usually has the form of:
jdbc:oracle:thin:@<tcp address>:<tcp port>:<database sid>.
For example to connect to the ORCL database on a machine using port 1521 you would use:
jdbc:oracle:thin:@206.168.191.19:1521:ORCL.

Note: The colon and @ symbols must be included as shown.

- You must specify the Oracle **Database Driver** that was installed on the SiteScope server when setting up the monitor. The Database Driver for the Oracle thin JDBC driver is:
oracle.jdbc.driver.OracleDriver
- You should only have one Oracle client installed on the SiteScope machine. If there is more that one client installed, SiteScope may report an error and be unable to connect to the database.

The default run schedule for this monitor is every 10 minutes, but you can change it to run more or less often using the **Frequency** setting.

Configuring the Oracle Database Monitor

The Oracle Database Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the Oracle Database Monitor.

Main Settings for the Oracle Database Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the Oracle database server, how often this Oracle Database Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Server

Enter the connection information for the server where the database you want to monitor is running.

Database Connection URL

Enter the connection URL to the database you want to monitor. For example, jdbc:oracle:thin:@206.168.191.19:1521:ORCL.

Database User Name

Enter the user name that SiteScope should use to connect to the database.

Database Password

Enter the password for the user name that SiteScope should use to connect to the database.

Database Driver

Enter the driver used to connect to the database. For example, oracle.jdbc.driver.OracleDriver.

Connection Timeout

Enter an optional the time out value, in seconds, that SiteScope should to wait for a database connection to respond. If the database connection can not be completed within the period specified, SiteScope will report an error.

Note: The sum of the Connection Timeout value and Query Timeout value should always be less than the Update every value for the monitor. For example, if the monitor Update every value is set to 10 minutes, this equates to 600 seconds.

Query Timeout

Enter an optional the time out value, in seconds, that SiteScope should to wait for a response from the database query. If the database does not respond within the period specified, SiteScope will report an error.

Note: The sum of the Connection Timeout value and Query Timeout value should always be less than the Update every value for the monitor. For example, if the monitor Update every value is set to 10 minutes, this is equivalent to 600 seconds. If both the Connection Timeout value and Query Timeout value are set to 120 seconds, the sum of these would be 240 seconds.

Note: Some commonly used databases and database drivers do not support the query timeout feature. In these cases the Query Timeout value should be set to zero.

Counters

You use the features associated with the **Counters** setting to choose and manage the metrics you want to monitor with the Oracle Database Monitor. Use the following steps to select and add counters.

To select or add counters:

1. Click **Get Counters** to query the remote system. After SiteScope has successfully connected to the remote system, the Get Counters selection dialogue opens.
2. Use the features in the Get Counters selection dialogue screen to select the Oracle database server metrics you want to monitor. Use the expandable menu controls as applicable to browse the available counters.
3. Use the check boxes to select between one and ten counters to be monitored.
4. Click **OK** to add the selected counters to the monitor configuration. The Get Counters selection dialogue closes and the monitor properties are updated with your selection.

Use the following steps to remove a counter from the selected counters list.

To remove or edit counters:

1. Click to edit the monitor for which you want to remove counters. Alternately, you may select the monitor you want to edit and click the Properties tab and click the **Edit** button. The monitor Properties screen opens.
2. Click the **Get Counters** button to open the Get Counters selection dialogue.
3. Clear the check box to the left of the current counter you want to remove.

   At this point, you may add other counters to the monitor by clicking the applicable check boxes.
4. Click **OK** at the bottom of the screen to update the monitor.

Name

Enter a text name for this Oracle Database monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the Oracle Database Monitor should server system check the Oracle database server. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Advanced Settings for the Oracle Database Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Oracle Database Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set one or more status thresholds criteria for each status condition per monitor instance. The status of the monitor and any associated alert action will be set based on comparison of all the threshold criteria you define for the monitor. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the Oracle Database or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the Oracle Database Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

51

Ping Monitor

The Ping Monitor checks the availability of a host via the network. Use this monitor to check that your connection to the Internet is available.

This chapter describes:	On page:
About the Ping Monitor	513
Configuring the Ping Monitor	514

About the Ping Monitor

The network can often be a Web traffic bottleneck, especially on relatively slow wide area network connections. The Ping Monitor obtains two of the most common measurements used to determine if your network connection is congested: Round Trip Time and Loss Percentage. An increase of either of these suggests that you are experiencing problems. In the case of Loss Percentage, you want to see a 0% reading. A 100% reading indicates your link is completely down. Some loss may happen very occasionally, but if it becomes common, the network is either flaky (some packets are being lost), or very busy and the router may be dropping the Ping packets.

Each time the Ping Monitor runs, it returns a reading and a status message and writes them in the monitoring log file. It also writes the total time it takes to receive a response from the designated host in the log file.

What to Monitor

We suggest that you set up monitors that test your connection to the Internet at several different points. For example, if you have a T1 connection to a network provider who in turn has a connection to the backbone, you would want to set up a Ping Monitor to test each of those connections. The first monitor would ping the router on your side of the T1. The second would ping the router on your provider's side of the T1. The third monitor would ping your provider's connection to the backbone.

In addition to these monitors, it is also a good idea to have a couple of other monitors ping other major network providers. These monitors will not really tell you whether the other provider is having a problem, but it will tell you if your network provider is having trouble reaching them.

About Scheduling this Monitor

Because it will not cost you much performance wise, you can monitor your own router as often as every two minutes or so. That way you will know about any problems on your end. The monitors that watch your provider's connection to your line and to the backbone should only be run every ten minutes or so. This will minimize traffic while still providing you with sufficient coverage.

Configuring the Ping Monitor

The Ping Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the Ping Monitor.

Main Settings for the Ping Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the remote system, how often this Ping Monitor instance should be run, and the text name used for this monitor instance. See “Common Monitor Settings” in the chapter “Working with SiteScope Monitors” for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this Ping monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the Ping Monitor should connectivity check the remote system. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Host Name

Enter the IP address or the name of the host that you want to monitor. For example, you could enter either 206.168.191.21 or demo.thiscompany.com.

Advanced Settings for the Ping Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Ping Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Time Out

This advanced option gives you the ability to customize the Ping Monitor's time out threshold -- the time that should pass before the ping times out. If you choose not to set it, SiteScope uses a pre-set default of 5000 milliseconds. To change the threshold, type the new value in the text box. The value must be in milliseconds.

Size

This advanced option gives you the ability to customize the size of the ping packets sent. If you choose not to set it, SiteScope uses a pre-set default of 64 bytes. To change the threshold, type the new value in the text box. The value is in bytes.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule

➤ Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set up to ten status thresholds criteria for each status condition per monitor instance. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the Ping or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the Ping Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

52

Port Monitor

The Port Monitor verifies that a connection can be made to a network port and measures the length of time it takes to make the connection. Optionally, it can look for a string of text to be returned or send a string of text once the connection is made.

This chapter describes:	On page:
About the Port Monitor	521
Configuring the Port Monitor	522

About the Port Monitor

The Port Monitor is useful for monitoring network applications that none of the other SiteScope monitors watch. You will be notified immediately if SiteScope is unable to connect to the monitored port.

What to Monitor

You can use the Port Monitor to watch those network applications that SiteScope does not specifically watch, such as Gopher and IRC services, some media services, or other custom network applications.

About Scheduling this Monitor

Scheduling Port monitors depends on the application or system you are monitoring. The Port Monitor does not use many resources, so you can schedule it to run as often as every 15 seconds if necessary. Monitoring most systems every 10 minutes is normally sufficient.

Status

Each time the Port Monitor runs, it returns a status message and writes them in the monitoring log file. It also writes the total time it takes to receive a response from the remote service.

The reading is the current value of the monitor. The possible values for the Port Monitor are:

- OK
- unknown host name
- unable to reach server
- unable to connect to server
- timed out reading
- match error

The status is logged as either good or error. An error status is returned if the current value of the monitor is anything other than OK.

Configuring the Port Monitor

The Port Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the Port Monitor.

Main Settings for the Port Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the remote system, how often this Port Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this Port monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the Port Monitor should remote port check the remote system. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Host Name

Enter the IP address or the name of the host that you want to monitor. For example, you could enter either 206.168.191.21 or demo.thiscompany.com.

Port Number

Choose the port number to connect to from the list of services, or enter a port number in the text box. Additional entries can be added to list by editing the master.config file in the **<SiteScope install path>/SiteScope/groups** directory.

Advanced Settings for the Port Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Port Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Send String

This advanced option gives you the ability to customize the string sent after a connection is made.

Match String

This advanced option gives you the ability to check for a string of text after a connection is made. If the text is not received, the monitor will display "no match on content". The search is case sensitive.

Timeout

The number of seconds that the Port monitor should wait for the connection to the port, and for any sending and receiving to complete. Once this time period passes, the Port monitor will log an error and report an error status.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set up to ten status thresholds criteria for each status condition per monitor instance. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the Port or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.

3 Enter a value applicable to the measurement parameter in the third text box.

4 To add another threshold setting, click the **New Error If** button and repeat the steps above.

5 Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the Port Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

53

Radius Monitor

The Radius Monitor checks that a RADIUS server is working correctly by sending an authentication request and checking the result. The word RADIUS is an acronym for Remote Authentication Dial In User Service and a RADIUS server is used to authenticate users, often connecting through a remote connection such as a dialup modem or a DSL line.

This chapter describes:	On page:
About the Radius Monitor	529
Configuring the Radius Monitor	530

About the Radius Monitor

The Radius Monitor is useful for testing that the RADIUS server is correctly handling authentication requests. If the RADIUS server fails, any users that try to use it will be unable to login and access any services. Setup a Radius monitor for each RADIUS server in your environment. You may want to setup multiple monitors per server if you want to test different kinds of login accounts.

In order for SiteScope to monitor your Radius server you must first add the IP address of your SiteScope server to the list of Clients that the Radius server is allowed to communicate with. This must be done in order for the Radius Server to take requests from SiteScope. Failure to do this will result in "Unknown Client" errors on the Radius Server.

The Radius Monitor currently supports Password Authentication Procedure (PAP) authentication but not the Challenge Handshake Authentication Protocol (CHAP) or Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) . Your RADIUS servers must be configured to accept PAP requests in order to use this monitor.

Status

Each time the Radius Monitor runs, it returns a status message and writes it in the monitoring log file. It also writes the total time it takes to receive a authentication response.

The reading is the current value of the monitor. The possible values for the Radius Monitor are:

- OK
- unknown host name
- timed out reading
- match error

The status is logged as either good or error. An error status is returned if the current value of the monitor is anything other than OK.

Configuring the Radius Monitor

The Radius Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the Radius Monitor.

Main Settings for the Radius Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the RADIUS server, how often this Radius Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this Radius monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the Radius Monitor should authentication system check the RADIUS server. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

RADIUS Server

Enter the IP address or the name of the RADIUS server that you want to monitor. For example, you could enter either 206.168.191.21 or radius.thiscompany.com.

Secret

Enter the secret used to encrypt all requests to this RADIUS server

Username

Enter the username to authenticate

Password

Enter the password to authenticate

Advanced Settings for the Radius Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Radius Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Timeout

The number of seconds that the Radius monitor should wait for the connection to the port, and for any sending and receiving to complete. Once this time period passes, the Radius monitor will log an error and report an error status.

Port Number

Choose the TCP port used by the RADIUS server. The default port used by RADIUS servers is 1645 and does not usually need to be changed

Match Content

Enter a string of text to check for in the response. If the text is not contained in the response, the monitor will display "no match on content". The search is case sensitive. You may also perform a regular expression match by enclosing the string in forward slashes, with an "i" after the trailing slash indicating case-insensitive matching. (for example, "/ \d\d/" or "/size \d\d/i").

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See “Common Monitor Settings” in the chapter “Working with SiteScope Monitors” for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set up to ten status thresholds criteria for each status condition per monitor instance. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the Radius or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the Radius Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

54

Real Media Player Monitor

The Real Media Player Monitor allows you to emulate a user playing media or streaming data from a Real Media Server. The error and warning thresholds for the monitor can be set on one or more Real Media Player performance statistics.

This chapter describes:	On page:
About the Real Media Player Monitor	537
Configuring the Real Media Player Monitor	538

About the Real Media Player Monitor

Use the Real Media Player Monitor to monitor availability and delivery quality parameters for media files and streaming data compatible with RealNetworks Real Media Players. You can monitor multiple parameters or counters with a single monitor instance. This allows you to report on delivery performance. Create a separate monitor instance for files or data streams that are representative of the content available from the site you want to monitor.

Before you can use the Real Media Player Monitor, Real Media Player client libraries must be installed on the server where SiteScope is running. Normally, it is sufficient to download and install a Real Media Player client on the server.

Configuring the Real Media Player Monitor

The Real Media Player Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the Real Media Player Monitor.

Main Settings for the Real Media Player Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the Real Media Player, how often this Real Media Player Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this Real Media Player monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the Real Media Player Monitor should player test the Real Media Player. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

URL

Enter the URL of the media file or streaming source you want to monitor. This should be the URL of the media file. This monitor does not support metadata files such as the .smi format.

Note: You should only monitor video, not audio, streams with this monitor.

Counters

Choose the media player performance parameters or counters you want to check with this monitor. The table list to the right of this item displays those currently selected for this monitor. Click **Get Counters** to bring up the counters selection screen. Check or clear the check boxes on the Get counters screen to select one or more counters to monitor on this server. The performance parameters or counters available for the Real Media Player Monitor include:

- stream quality
- live pause num
- live pause time
- buffering congestion num
- buffering congestion time
- buffering seek time
- buffering seek num
- buffering time
- buffering num
- first frame time
- network performance
- bandwidth
- late packets
- lost packets
- recovered packets

Duration

Enter the playback duration (in milliseconds) that the monitor should use for the media file or source indicated by the **URL** above. The duration value does not need to match the duration of the media contained in the file. For example, you can direct SiteScope to monitor a media file that contains 45 seconds of media content. The default **Duration** for the Real Media Player Monitor is 15000 milliseconds which equals 15 seconds. In this

configuration, the monitor instance would connect to the media source and play the media content for 15 seconds and report the status for those 15 seconds. If the media content of the file or source you are monitoring is less than the **Duration** value selected for the monitor, the monitor plays the entire media content and reports the results, including the time required to play the media content.

Advanced Settings for the Real Media Player Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Real Media Player Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set one or more status thresholds criteria for each status condition per monitor instance. The status of the monitor and any associated alert action will be set based on comparison of all the threshold criteria you define for the monitor. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the Real Media Player or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the Real Media Player Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

55

Real Media Server Monitor

The Real Media Server Monitor allows you to monitor the availability of an Real Media Server on Windows NT systems. The error and warning thresholds for the monitor can be set on one or more Real Media Server performance statistics.

This chapter describes:	On page:
About the Real Media Server Monitor	545
Configuring the Real Media Server Monitor	546

About the Real Media Server Monitor

Use the Real Media Server Monitor to monitor the server performance parameters for RealNetworks Real Media Servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate monitor instance for each RealSystem Server you are running.

The Real Media Server Monitor makes use of Performance Counters to measure application server performance. SiteScope will need to be running under an account that has the necessary administrative security privileges to access performance counter data from remote servers. If the servers you want to monitor are in a different domain, are governed under a different policy, or require a unique login different than the account SiteScope is running under, then you will need to define the connection to these servers under the NT Remote Preferences option in the SiteScope Preferences container.

The Remote Registry service must be running on the machine where the Real Media server is running if the Real Media Server is running on Windows 2000.

The default run schedule for this monitor is every 10 minutes, but you can change it to run more or less often using the **Frequency** setting.

Configuring the Real Media Server Monitor

The Real Media Server Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the Real Media Server Monitor.

Main Settings for the Real Media Server Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the Real media server, how often this Real Media Server Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this Real Media Server monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the Real Media Server Monitor should server performance check the Real media server. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Server

Choose the server where the Real Media Server you want to monitor is running. Use the drop-down list to select a server from the list of remote servers that are available to the SiteScope agent.

Counters

You use the features associated with the **Counters** setting to choose and manage the metrics you want to monitor with the Real Media Server Monitor. Use the following steps to select and add counters.

To select or add counters:

1. Click **Get Counters** to query the remote system. After SiteScope has successfully connected to the remote system, the Get Counters selection dialogue opens.
2. Use the features in the Get Counters selection dialogue screen to select the Real media server metrics you want to monitor. Use the expandable menu controls as applicable to browse the available counters.
3. Use the check boxes to select between one and ten counters to be monitored.
4. Click **OK** to add the selected counters to the monitor configuration. The Get Counters selection dialogue closes and the monitor properties are updated with your selection.

Use the following steps to remove a counter from the selected counters list.

To remove or edit counters:

1. Click to edit the monitor for which you want to remove counters. Alternately, you may select the monitor you want to edit and click the Properties tab and click the **Edit** button. The monitor Properties screen opens.
2. Click the **Get Counters** button to open the Get Counters selection dialogue.
3. Clear the check box to the left of the current counter you want to remove.

   At this point, you may add other counters to the monitor by clicking the applicable check boxes.
4. Click **OK** at the bottom of the screen to update the monitor.

The performance parameters or counters available for the Real Media Server Monitor include:

- Encoder Connections
- HTTP Clients
- Monitor Connections
- Multicast Connections
- PNA Clients
- RTSP Clients
- Splitter Connections
- TCP Connections
- Total Bandwidth
- Total Clients
- UDP Clients

Advanced Settings for the Real Media Server Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Real Media Server Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set one or more status thresholds criteria for each status condition per monitor instance. The status of the monitor and any associated alert action will be set based on comparison of all the threshold criteria you define for the monitor. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the Real Media Server or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the Real Media Server Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

56

Real Time Streaming Protocol Monitor

The Real Time Streaming Protocol (RTSP) Monitor can be used to check the availability of certain kinds of time-based media files and real-time media streams (see table below for examples of supported formats).

This chapter describes:	On page:
About the RTSP Monitor	553
Configuring the RTSP Monitor	557

Note: The RTSP Monitor does not support Real Media file types (for example: *.ra, *.ram files) or Windows Media files (for example: *.asf files). Use the Real Media Server and Real Media Player monitors or the Windows Media Server and Windows Media Player monitors to monitor these types of services.

About the RTSP Monitor

You use the RTSP Monitor to check the availability of a media source or media file, check that it can be retrieved, that the file is complete, and that the download rate meets your requirements.

UNIX and Linux Requirements

For SiteScope on UNIX or Linux, the RTSP Monitor requires that an X11 server be available. If SiteScope is unable to contact the X11 server specified by the DISPLAY environment variable then it will not be able to load the JMF player used by this monitor and will issue a "Player Create Error". The DISPLAY environment variable must be set prior to starting SiteScope. For convenience this variable can be set in the SiteScope user's login environment scripts.

The following are three options for meeting the configuration requirement for the RTSP Monitor on UNIX and Linux:

1. Log into the graphical system console, execute xhost +locahost, and set your DISPLAY variable to the appropriate value before starting SiteScope. You must remain logged into the graphical console to maintain the X11 server active. If you log out of the console session, the X11 server will shutdown and the RTSP Monitor will not be able to contact it.
2. Run a PC X11 server such as Exceed, and specify the appropriate value for DISPLAY prior to starting SiteScope. The X11 server process (such as Exceed), must be running as long as SiteScope is running. If the RTSP Monitor is unable to contact the X11 server it will generate a "Player Create Error".
3. Install and run Xvfb, the X Virtual Frame Buffer on your UNIX/Linux system. Xvfb is an X11 server emulator which can be run as a daemon and will meet the X11 server requirements of the RTSP Monitor. Most Linux distributions include Xvfb, and it is also available on Solaris 9. For earlier Solaris versions you will need to download the X11R6 source code from ftp.x.org. After installing Xvfb, a startup script can be configured to start Xvfb on system boot with a command similar to the following:

   ```
   /path_to_xvfb/Xvfb :77 > /dev/null 2>&1 &
   ```

   The :77 parameter tells Xvfb to run on display number 77. In this example we would need to set our display variable to hostname:77

   The advantage of Xvfb over the other two options is that it provides a working X11 server without requiring that a user be logged into a system console on either an NT or UNIX system.

The RTSP Monitor makes use of the Java Media Framework (JMF) which provides the capability of monitoring a variety of real time digital media types and protocols. This includes HTTP retrieval of media files and RTSP streaming of many types of files. The table below is an overview of the media formats that have some support in the RTSP Monitor.

Note: Due to the many variations of media recording options not all files of the types listed below are supported by the Java Media Framework and RTSP Monitor. For example, some MP3 and MOV options are not supported. We recommend that you test a variety of files with the RTSP Monitor to determine if the file format you want to monitor can be decoded by the RTSP Monitor

---

Media Type	**File Format**
Audio Interchange File Format (Apple)	***.aiff**
Audio Video Interleave (Microsoft)	***.avi**
Flash (Macromedia)	***.swf, *.spl**
Global Standard for Mobile Communications GSM (wireless telephony standard)	***.gsm**
HotMedia (IBM)	***.mvr**
Musical Instrument Digital Interface (MIDI)	***.mid**
Motion **P**icture **E**xperts **G**roup MPEG-1 Video	***.mpg**
MPEG Layer II Audio	***.mp2**
MPEG Layer III Audio	***.mp3**
QuickTime Movie (Apple)	***.mov**

Sun Audio (Sun Microsystems)	***.au**
Wave audio file format (Microsoft)	***.wav**

A more complete list of supported media types can be found at: http://java.sun.com/products/java-media/jmf/2.1/formats.html#RTPFormats

---

Note: The SiteScope RTSP Monitor **does not** support RealMedia formats from RealNetworks. In order to monitor RealMedia servers and media formats, see the Real Media Server Monitor or Real Media Player Monitor.

This monitor should be set to run according to your reasonable acceptable error period. The utilization of monitoring bandwidth and overall monitoring system performance should be considered in setting the run interval for this type of monitor. The default run interval is set to 10 minutes.

Status

Each time a RTSP Monitor runs, it attempts to open and read a specified media stream or download and play a specified media file. The monitor records a status and stream or file statistics when the session is completed. If the file or stream is not supported or is unavailable, an error is reported.

Each time the monitor runs it returns a status which includes the current value of the monitor. The possible status values are:

- OK
- warning
- error

The final status result is either OK, error, or warning based on threshold established for these conditions.

Configuring the RTSP Monitor

The RTSP Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the RTSP Monitor.

Main Settings for the RTSP Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the media files or streams, how often this RTSP Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this RTSP monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the RTSP Monitor should media test the media files or streams. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Media URL

Enter the URL of the media file (for HTTP download and playback) or the URL of the media stream (for RTSP streaming) to be tested.

Note: It is important to note that the SiteScope RTSP Monitor may not process media reference files or media metadata files that are commonly used with RealNetworks RealPlayer reference files and with some QuickTime movies.

Advanced Settings for the RTSP Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the RTSP Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Time Out

This advanced option gives you the ability to customize the RTSP Monitor's time out threshold. The Timeout is the time that should pass before the RTSP Monitor process is timed out. If you choose not to set it, SiteScope uses a pre-set default of 60000 milliseconds. To change the threshold, type the new value in the text box. The value must be in units of milliseconds.

Note: In order to test media files to completion, the **Timeout** value should be set to a value greater than the time that it should take to playback the subject media download. For example, if the media file should normally playback in 90 seconds, the Timeout value should be set for greater than 90 seconds.

Stop Time

This advanced option gives you the ability to stop the media download after some specified amount of time has elapsed. Setting the value of 0 will cause the media stream to download until end of media is detected. Using a value greater than zero will stop the download of continuous broadcast streams (such as radio station multicasts) or very large media downloads.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set up to ten status thresholds criteria for each status condition per monitor instance. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the RTSP or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the RTSP Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

57

SAP Monitor

The SAP Monitor allows you to monitor the availability and performance statistics of a SAP Application Server. The error and warning thresholds for the monitor can be set on as many as ten SAP server performance statistics.

This chapter describes:	On page:
About the SAP Monitor	563
SAP Java Connector Installation	564
Configuring the SAP Monitor	565

About the SAP Monitor

Use the SAP Monitor to monitor the server performance data for SAP application servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate monitor instance for each SAP server in your environment.

The default run schedule for this monitor is every 10 minutes, but you can change it to run more or less often using the **Frequency** setting.

To enable the SAP monitor, you must install the SAP Java Connector. For details, see below.

SAP Java Connector Installation

The SAP monitor uses SAP JCo libraries to connect to the SAP R/3 system. A user must have the appropriate license granted by SAP to receive and use these libraries.

To enable the SAP monitor on a Windows environment:

1 Download the following .jar file and .dll files from the SAP support Web site:

- **sapjco.jar**
- **librfc32.dll**
- **sapjcorfc.dll**

2 Copy the **sapjco.jar** file into the **<SiteScope root directory>/WEB-INF/lib** directory.

3 Copy the two .dll files into the **<SiteScope root directory>/bin** directory.

Note: Check if the .dll files already exist in your **<Windows installation directory>/system32** directory. They may have been copied into this directory as part of the SAP client installation. If they do exist in your system, you must overwrite them with the above .dll files before copying into the SiteScope directory.

---

4 Restart SiteScope.

To enable the SAP monitor on a UNIX environment:

1 Download the following .jar file and .so files from the SAP support Web site:

- **sapjco.jar**
- **librfccm.so**
- **libsapjcorfc.so**

2 Copy the **sapjco.jar** file into the **<SiteScope root directory>/WEB-INF/lib** directory.

3 Copy the two .so files as follows:

- For Sun installations, copy into the **<SiteScope root directory>/java/bin/sparc** directory.
- For Linux installation, copy into the **<SiteScope root directory>/java/bin/i386** directory.

4. Restart SiteScope.

Configuring the SAP Monitor

The SAP Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the SAP Monitor.

Main Settings for the SAP Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the SAP application system, how often this SAP Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this SAP monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the SAP Monitor should system check the SAP application system. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Server

Enter the address of the SAP server you want to monitor. If the connection is being made through a router, it may be necessary to enter the router address string as part of the server address. For example: /H/199.35.102.8/H/205.78.199.235/H/<servername>. You can find the router address using the SAP Logon tool from the SAP Client software. Open the Logon console, select the server you want to monitor and then select **Properties** to view the router address.

Application Server

Enter the address of the SAP server you want to monitor.

SAP Client

Enter the Client to use for connecting to SAP.

System Number

Enter the System number for the SAP server.

Authorization User Name

Enter the user name required to connect to the SAP server.

Authorization Password

Enter the password required to connect to the SAP server.

SAP Router String

If your connection is being made through a router, enter a router address string. You can find the router address using the SAP Logon tool from the SAP Client software. Open the Logon console, select the server you want to monitor and then select **Properties** to view the router address. Leave it blank otherwise.

Counters

You use the features associated with the **Counters** setting to choose and manage the metrics you want to monitor with the SAP Monitor. Use the following steps to select and add counters.

To select or add counters:

1. Click **Get Counters** to query the remote system. After SiteScope has successfully connected to the remote system, the Get Counters selection dialogue opens.
2. Use the features in the Get Counters selection dialogue screen to select the SAP application system metrics you want to monitor. Use the expandable menu controls as applicable to browse the available counters.
3. Use the check boxes to select between one and ten counters to be monitored.
4. Click **OK** to add the selected counters to the monitor configuration. The Get Counters selection dialogue closes and the monitor properties are updated with your selection.

Use the following steps to remove a counter from the selected counters list.

To remove or edit counters:

1. Click to edit the monitor for which you want to remove counters. Alternately, you may select the monitor you want to edit and click the Properties tab and click the **Edit** button. The monitor Properties screen opens.
2. Click the **Get Counters** button to open the Get Counters selection dialogue.
3. Clear the check box to the left of the current counter you want to remove.

   At this point, you may add other counters to the monitor by clicking the applicable check boxes.
4. Click **OK** at the bottom of the screen to update the monitor.

Some of the performance objects and counters available for the SAP Monitor include:

- Average CPU time
- Average response time
- Average wait time
- Average load time
- Database calls

- Database requests
- GUI time
- Roll ins
- Roll outs
- Roll in time
- Roll out time
- Roll wait time
- Average time per logical DB call

Advanced Settings for the SAP Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the SAP Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set one or more status thresholds criteria for each status condition per monitor instance. The status of the monitor and any associated alert action will be set based on comparison of all the threshold criteria you define for the monitor. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the SAP or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the SAP Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- ➤ Do not report to Mercury Business Availability Center
- ➤ Report everything (all monitors and all measurements)
- ➤ Report monitor level data (no measurements)
- ➤ Report monitor level data and measurements with thresholds
- ➤ Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

58

Script Monitor

The Script Monitor runs an external command and reports the result. It is one way to integrate existing system management scripts into the SiteScope environment. The Script Monitor can be tailored to run scripts at regular intervals. In addition to reporting the command result, the Script Monitor can also parse and report a specific value from the command output.

This chapter describes:	On page:
About the Script Monitor	573
Configuring the Script Monitor	576
Script Return Status Example	583
Setting a Timeout Value for Script Execution	584

About the Script Monitor

One of the primary reasons for using the Script Monitor is to integrate an existing script that you use to do a particular system management function into SiteScope. For example, if you have a script that runs a diagnostic on an application and returns a 0 reading if everything's OK, you could create a script monitor that runs this script and recognizes any exit value other than 0 as an error. Then you could create an alert which would e-mail or page you in the event that this monitor was in error.

The Script Monitor can be used to run shell commands or other scripts on the machine where SiteScope is running or it can run a script that is stored on a remote machine. The following is an overview of the possible script execution options and requirements for the SiteScope Script Monitor:

Script Option	Description
Local Script	A file stored and executed on the SiteScope machine. The file should be stored in the **<SiteScope install path>/SiteScope/scripts** directory.
Remote Script	A remote script file (UNIX and Windows-Windows SSH ONLY) in a scripts subdirectory in the home directory of the account SiteScope uses to access the remote server. For example, home/sitescope/scripts. The remote scripts must include an echo construct to echo script results and exit codes back to SiteScope (see the Return Status Example section below). The monitor may fail if the appropriate exit code is not echoed back to SiteScope.
Remote Command	A script file containing a single command stored locally in the **<SiteScope install path>/SiteScope/scripts.remote** directory. This script file is used to run a command on a remote server. The command may be used to execute a remote script file that performs multiple functions.

Note: For SiteScope on Linux, the script itself must have a shell invocation line as the very first line of the script. This applies to scripts that you are trying to run locally on the SiteScope machine. For example, the first line of the script should include something like #!/bin/sh or #!/usr/local/bin/perl. If the shell invocation line is not found then the exec() call will return with a -1 exit status. This is a limitation of the Java Runtime in JRE prior to release 1.4. This has been fixed in the 1.4 JRE from Sun which is shipped with SiteScope version 7.8 and later.

Scheduling Script monitors is dependent upon the script that you want SiteScope to run. You can use the scheduling option to have SiteScope run scripts at different intervals throughout the week.

Status

Each time the Script Monitor runs, it returns a status and writes it into the monitoring log file. It also reports a command result, a value, and the time it took to run the command.

The command result is the exit value returned by running the command. This works for local UNIX scripts, but does not work for remote UNIX scripts, or Win NT batch files. Win NT batch file (*.bat) exit codes are not passed out of the command interpreter, and remote UNIX script exit codes are not passed back through the remote connection. See the example below for a way to receive information from the script.

Caching Script Output

The Script Monitor includes an optional feature that can be used to cache the output of a script execution. The cached output is useful in you want to:

- have multiple script monitors check and alert on different parts of the output of a script
- reduce network traffic and server load by minimizing the number of times a script is executed

You can enable script output caching by entering a time value (in seconds) greater than zero in the **Cache Life** setting in the Advanced Settings section. In order to configure multiple Script monitors to use the data in the cache you must ensure that each monitor instance:

- is configured to use the same remote Server profile
- is configured to use the same Script file
- has a **Cache Life** value greater than zero

The **Cache Life** value entered for each monitor should approach, but not exceed, the equivalent of the value selected for the **Frequency** setting for that monitor. For example, if the **Frequency** setting is 10 minutes, the **Cache Life** value can be set to a value of 590 since 10 minutes is equivalent to 600 seconds and 590 is less than 600. Any monitor that detects the end of its Cache Life will run the script again and refresh the cache.

Configuring the Script Monitor

The Script Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the Script Monitor.

Main Settings for the Script Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the remote system, how often this Script Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this Script monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the Script Monitor should script execution the remote system. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Script

Enter the name of the script to run. For security reasons, only scripts placed into the **<SiteScope install path>/SiteScope/scripts** directory may be used. In that directory, there are several examples scripts with comments describing each one.

If you choose "USE COMMAND", your must also specify a USE COMMAND script file name in the Advanced Settings section below. SiteScope will send the command or commands found in the USE COMMAND script file to be executed as a command line on the remote UNIX Machine. Script files for the USE COMMAND option must be created in the **<SiteScope install path>/SiteScope/scripts.remote** directory.

For Example, create a file named **test.sh** and save it in the **<SiteScope install path>/SiteScope/scripts.remote directory**. Edit **test.sh** to include the command syntax ps -ef;echo "all done" as the content of the file. Then create a Script monitor with the USE COMMAND option selected, select a remote UNIX machine, and select test.sh as the USE COMMAND script to run.

Server

By default, SiteScope will execute script files that are stored locally on the SiteScope machine in the **<SiteScope install path>/SiteScope/scripts** directory. You can have SiteScope execute a script that is stored on a remote machine by selecting the remote machine using the drop-down list to select a server from the list of remote servers that are available to the SiteScope agent. If the remote machine you are looking for does not appear in the list, you will need to create a connection profile using the Remote UNIX Preferences page.

Parameters

Use this text box to specify any additional parameters to pass to the script. Optionally, you can use a regular expression or one of SiteScope's date variables to insert date and time into the parameters box. For example, s/$month$ day $year$/ will pass the current month, day and year to the script.

Note: For security reasons the following characters are not allowed to be passed to scripts by SiteScope:` (apostrophe), ; (semicolon), & (ampersand), | (vertical pipe), < (less than), > (greater than).

Advanced Settings for the Script Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Script Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

USE COMMAND Script File

If you have selected the USE COMMAND as the **Script** option above and a remote machine as the **Server**, select the script file that contains the commands that SiteScope should send to the remote machine. You can save one or more commands in the text script file and save the file in the **<SiteScope install path>/SiteScope/scripts.remote** directory. SiteScope will open this file and run the command at the command line of the remote server chosen in the "choose server" option above. You can then use the **Match Expression** option to parse the output of the command and display valuable information.

The USE COMMAND script can make use of positional parameters such as $1, $2 (or alternatively %1, %2), and so forth, inside the script. Enter the parameters you want SiteScope to pass to the script in the **Parameters** box provided above.

Note: You can use one or more commands per USE COMMAND script file. **DO NOT** include any carriage returns or any command that would normally discontinue script processing (for example, do not use the exit command).

Cache Life

You use this option only if you want to use multiple Script monitor instances to check or match on content returned by a single run of a script. Enter a time value (in seconds) greater than zero to have SiteScope cache the output of the script execution. Each time the monitor is run SiteScope will check if the cache life has expired. If it has not then the monitor will use the cached script output data, otherwise the script will be executed again to update the cache and the monitor. Enter a value of 0 (zero) to disable the cache function. This will cause the monitor to execute the script each time that it runs.

Match Expression

To retrieve a value from the script output, enter a regular expression in this box. For example, the expression: /(\d+)/ will match one or more digits returned by the script. The retrieved value can be used to set the error or warning status of the monitor and to trigger alerts. SiteScope will check up to four values returned. If this item is left blank, no value will be retrieved from the script.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set up to ten status thresholds criteria for each status condition per monitor instance. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the Script or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the Script Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

Script Return Status Example

In order to get around the fact that exit codes that are not returned to SiteScope after execution of Win NT batch files or UNIX scripts executed on remote servers, we recommend including an echo to standard out of a return value. In the case of Win NT-to-NT remote scripts (using Secure Shell), the remote script MUST echo end script when the script has terminated. Other returned values can then be matched in the Script monitor using a regular expression in the **Match Expression** box.

The following is an example script outline based on a UNIX shell script.

In the script that will run on a remote server include echo commands that represent the different logical paths that might be followed:

#!/bin/sh
...(script commands and logic here)...
echo "Return Code: 1" (indicating the script failed to complete execution)
...(more script commands and logic here)...
echo "Return Code: 0" (the end of the script, indicating the script completed successfully)

Under the Advanced Settings in the Script Monitor set up page, create a Match Expression using the following regular expression pattern:

/Return Code: (\d+)/

Then set the Error, Warning, and Good thresholds for the monitor as follows:

Error if value > 0
Warning if value == 'n/a'
Good if value == 0

With this set up, if the echoed Return Code value is greater than 0, it signals that the script did not execute correctly. If the script does not run properly, meaning that no Return Code echo command in the script is executed, then a warning condition occurs (for example, there will not be a match for the Match Expression which will return a 'n/a'). If the script echoes the Return Code of 0, then a good condition is detected. In this case the monitor status shown on the monitor detail page will display "matched 0" if the script executed successfully.

Setting a Timeout Value for Script Execution

You can set a timeout value for the Script Monitor for SiteScope running on Windows. The timeout value is the total time, in seconds, that SiteScope should wait for a successful run of the script. You can use this option to have SiteScope run the monitor but kill the script execution if a script exit code is not detected within the timeout period.

The requirements and limitations of this option are:

- is only available with SiteScope for Windows
- can only be used with scripts stored and invoked on the local SiteScope server (that is, where the **Server** setting for the Script Monitor is this server or localhost)
- the timeout setting value is expressed in seconds
- only applies to Script Monitors

Two methods exist for applying a timeout setting to Script monitors. One applies the setting as a property to an individual monitor. The second method adds the setting to groups, subgroups, or the entire SiteScope installation. The procedures for both are described below.

To set a Timeout Value for Individual Script Monitors:

1. Stop the SiteScope service.
2. Using a text editor, open the SiteScope group file containing the monitor frame for the Script Monitor to which you want to apply the timeout setting.
3. Inside the Script Monitor frame (delimited by the # sign), insert a line and add the timeout setting as _timeout=time where time is replaced with the time in seconds.
4. Save the group file.

Note: Do not add blank lines, leading or trailing spaces to any record in the group file.

---

5. Restart the SiteScope service.

To set a Timeout Value for Multiple Script Monitors:

1. Stop the SiteScope service.
2. Using a text editor, open the SiteScope group file containing one or more Script monitors to which you want to apply the timeout setting. Alternately, you can add the setting to the **SiteScope/groups/master.config** file.
3. Inside the group file frame a the top of the file before the first # symbol, insert a line and add the timeout setting as _scriptMonitorTimeout=time where time is replaced with the time in seconds.
4. Save the group file.

Note: Do not add blank lines, leading or trailing spaces to any record in the group file or master.config file.

---

5. Restart the SiteScope service.

59

Service Monitor

The Service Monitor checks to see if a service (Windows environment) or a specific process (UNIX and Windows) is running. There are many services or processes that play an important role in the proper functioning of your server, including Web server, Mail, FTP, News, Gopher, and Telnet. Web environments which support e-commerce transactions may have other important processes that support data exchange.

This chapter describes:	On page:
About the Service Monitor	587
Configuring the Service Monitor	588

About the Service Monitor

The Service Monitor verifies that specific processes are listed as running, and optionally, it can also check to see how much CPU a process is using. If a process that should be running does not show up or if it is using too much memory, SiteScope can either alert you to the problem so that you can address it yourself, or it can run a script to automatically restart the process to help minimize impact on other operations and downtime.

What to Monitor

You should create a service monitor for any service or process that should be running on a consistent basis. You can also create a script alert that will restart the service automatically if the service monitor in SiteScope can not find it. The restartService.bat script, located in the **<SiteScope install path>/SiteScope/scripts** directory, is a template which you can customize to create a script for SiteScope to execute in the event your monitor fails.

About Scheduling this Monitor

The Service Monitor does not put a heavy load on your server. For monitoring remote UNIX servers, SiteScope will usually need to open a telnet or SSH connection to the remote server. While the monitor actions generally do not load the either server, managing a large number of remote connections can results in some performance problems. You will probably want to monitor critical services and services that have a history of problems every five minutes or so. Less critical services and processes should be monitored less frequently.

Status

Each time the Service Monitor runs, it returns a reading and a status message and writes them in the monitoring log file.

The reading is the current value of the monitor. For this monitor, the possible readings are:

- Running
- Not found

The status is logged as either OK or error. An error status is returned if the service is not found.

Configuring the Service Monitor

The Service Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the Service Monitor.

Main Settings for the Service Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the remote service or process, how often this Service Monitor instance should be run, and the text name used for this monitor instance. See “Common Monitor Settings” in the chapter “Working with SiteScope Monitors” for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this Service monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the Service Monitor should service or process check the remote service or process. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Server

Choose the server that you want to monitor. The default is to monitor services on the server on which SiteScope is installed. Use the drop-down list to select a server from the list of remote servers that are available to the SiteScope agent.

Service

Select the service (or process in UNIX) that you want to monitor from the drop-down list. To monitor a service other than those listed then select "Other" in the drop-down list and enter the name of the service in the text box to the right. To monitor an NT process, select "(Using Process Name)" in the drop-down list and enter the name of the **Process Name** text box under the Advanced Settings section.

Advanced Settings for the Service Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Service Monitor and its display in the product interface. See “Common Monitor Settings” in the chapter “Working with SiteScope Monitors” for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Process Name (NT Only)

If you want to get information about the percentage of CPU being used by a specific process and/or the number of a specific type of process running, enter the name of the process here. SiteScope is looking for the name of the process as it appears in NT Task Manager (example: explorer.exe).

Measure Process Memory Use (UNIX Only)

Check this box if you want SiteScope to report the amount of virtual memory being used by a specific process.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule

➤ Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

➤ Enable all associated alerts

➤ Disable all associated alerts for the next time period

➤ Disable all associated alerts on a one time schedule

➤ Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set up to ten status thresholds criteria for each status condition per monitor instance. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the Service or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the Service Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)

- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

60

SilverStream Server Monitor

The SilverStream Server Monitor allows you to monitor the availability of an SilverStream server. The error and warning thresholds for the monitor can be set on one or more SilverStream server performance statistics.

This chapter describes:	On page:
About the SilverStream Server Monitor	595
Configuring the SilverStream Server Monitor	596

About the SilverStream Server Monitor

Use the SilverStream Server Monitor to monitor the server performance metrics pages for SilverStream servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate monitor instance for each SilverStream server you are running.

You will need to know the server statistics URL for the SilverStream server you want to monitor. For some server configurations, you must use the server name rather than the IP address for the server.

The default run schedule for this monitor is every 10 minutes, but you can change it to run more or less often using the **Frequency** setting.

Configuring the SilverStream Server Monitor

The SilverStream Server Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the SilverStream Server Monitor.

Main Settings for the SilverStream Server Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the SilverStream server, how often this SilverStream Server Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this SilverStream Server monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the SilverStream Server Monitor should server check the SilverStream server. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

URL

Choose the URL you want to verify with this monitor. This URL should be the URL to the applicable server administration Web page which usually has the form of http://*servername:port*/SilverStream/Statistics. The default port number is port 80.

Counters

Select the server performance parameters or counters you want to check with this monitor. The table list to the right of this item displays those currently selected for this monitor. Click **Get Counters** to bring up the counters selection screen. Check or clear the check boxes on the Get Counters screen to select one or more counters to monitor on this server. The performance parameters or counters available for the SilverStream Server Monitor include:

- hits
- bytes
- Request processing times(min)
- Request processing times(avg)
- Request processing times(max)
- Thread counts(free)
- Thread counts(idle)
- Thread counts(total)
- Memory status(Free memory)
- Memory status(Total memory)
- Memory status(GC Count)
- Current load
- Session/License status(Idle sessions)
- Session/License status(Total sessions)
- Session/License status(Used licenses)
- Session/License status(Total licenses)

Advanced Settings for the SilverStream Server Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the SilverStream Server Monitor and its display in the product interface. See “Common Monitor Settings” in the chapter “Working with SiteScope Monitors” for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Timeout

The number of seconds that the monitor should wait for a response from the server before timing-out. Once this time period passes, the monitor will log an error and report an error status.

HTTP Proxy

Optionally, a proxy server can be used to access the server. Enter the domain name and port of an HTTP Proxy Server.

Authorization User Name

If the server you want to monitor requires a name and password for access, enter the name in this box.

Authorization Password

If the server you want to monitor requires a name and password for access, enter the password in this box.

NT Challenge Response

Check this box if you want SiteScope to use Window's NT Challenge Response authorization when accessing.

Proxy Server User Name

If the proxy server requires a name and password to access the server, enter the name here. Technical note: your proxy server must support Proxy-Authenticate for these options to function.

Proxy Server Password

If the proxy server requires a name and password to access the server, enter the password here. Technical note: your proxy server must support Proxy-Authenticate for these options to function.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set one or more status thresholds criteria for each status condition per monitor instance. The status of the monitor and any associated alert action will be set based on comparison of all the threshold criteria you define for the monitor. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the SilverStream Server or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1 Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.

2 Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.

3 Enter a value applicable to the measurement parameter in the third text box.

4 To add another threshold setting, click the **New Error If** button and repeat the steps above.

5 Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the SilverStream Server Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see “Common Monitor Settings” in the chapter Chapter 2, “Working with SiteScope Monitors.”

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see “Working with Categories” in *Working with Monitor Administration*.

61

SNMP Monitor

The SNMP Monitor reads a value from an SNMP device. Many network devices support the SNMP protocol as a way of monitoring them. You will need to know the OIDs (Object ID's) for the device you want to monitor. These may be available in the product documentation or in the form of a MIB file.

This chapter describes:	On page:
About the SNMP Monitor	605
Configuring the SNMP Monitor	606

Note: To have SiteScope listen for SNMP traps from multiple devices, use the SNMP Trap Monitor.

About the SNMP Monitor

Use the SNMP Monitor to monitor devices that communicate with the SNMP protocol, such as firewalls, routers and UPS's. Several operating systems suppliers also provide SNMP agents and Management Information Bases (MIB's) for accessing workstation or server performance metrics, interface statistics, and process tables via SNMP.

You can use the SNMP Monitor to watch any values known by the SNMP agent running on a device provided you can supply an OID that maps to that value. If your router supports SNMP, for example, you could have SiteScope monitor for packet errors, bandwidth, or device status.

Requirements for using the SNMP Monitor include:

- SNMP agents must be deployed and running on the servers and devices that you want to monitor
- The SNMP agents must be supplied with the necessary Management Information Bases (MIB's) and configured to read those MIB's
- You need to know the Object ID's (OIDs) of the parameters you want to monitor.

In some cases, an equipment manufacturer may supply a list of OIDs that are available. Otherwise, you may need to locate a MIB browser utility in order to "walk" a MIB and extract the values of interest to you.

You can also check the on-line Knowledge Base available via the Customer Support site for other information relating to monitoring SNMP systems.

Configuring the SNMP Monitor

The SNMP Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the SNMP Monitor.

Main Settings for the SNMP Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the network component, how often this SNMP Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this SNMP monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the SNMP Monitor should system check the network component. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Host Name

Enter the host name or IP address of the SNMP device that you want to monitor (for example, demo.thiscompany.com). By default, this will connect to port 161. If your SNMP device is using a different port, add it to the hostname using ":port". For example, to use port 170, you would enter demo.sitescope.com:170.

Object ID

Select the Object ID mnemonic from the drop-down list or enter the Object Identifier (OID) for the SNMP value you want to retrieve. The OID specifies which value should be retrieved from the device. (for example, 1.3.6.1.2.1.4.3). To troubleshooting basic connectivity to the device and to confirm that the SNMP agent is active, select the system.sysDescr object from the drop-down list if other objects can not be found.

Note: SiteScope version 7.1 and later supports SNMP version 1 and version 2. In order to send a trap using snmpv2, you must select the version number in the Advanced Settings section.

If you receive the error message "**There is no such variable name in this MIB**", it means SiteScope was able to contact the device but the OID given is not know by the device. You need to provide an OID that is valid to the device in order to obtain a value.

If you have a MIB file for the device you want to monitor, you can copy the *.mib (or *.my) file into the **<SiteScope install path>/SiteScope/templates.mib** subdirectory and use the MIB Help utility to compile the MIB and browse the OIDs for the device. Click the MIB Help hyperlink to bring up the MIB Helper. Select the MIB file to browse using the drop-down list. Click the **List OIDs** button to show the OIDs from the select MIB file

---

Note: It is not necessary to browse a MIB file with the SiteScope Mib Helper in order to monitor a device. The MIB Helper is provided simply as a tool to help you discover OIDs available on a device, but it is not the only tool available.

You can also check the on-line Knowledge Base available via the Customer Support site for other information relating to monitoring SNMP systems. Also note that not all MIB files can be browsed by the MIB Helper: the Mib Helper only supports MIB files that are version SNMP v1.

Index

The index of the SNMP object. Values for an OID come as either scalar or indexed (array or table) values. For a scalar OID, the index value must be set to 0. For an indexed or table value, you must provide the index (a positive integer) to the element that contains the value you want. For example, the OID 1.3.6.1.2.1.2.2.1.17 is an indexed value that contains four elements. To access this second element of this OID you enter an index of 2 in the **Index** text box. To access the fourth element, enter an Index value of 4.

In some vendor specific MIB's, the indexed entries (often referred to in tables) can have compound index values. For example, the OID for the process entry table in a Sun MicroSystems server MIB may be: .1.3.6.1.4.1.42.3.12.1.1. This indexed or table object may have up to eleven nodes with OIDs ranging from .1.3.6.1.4.1.42.3.12.1.1.1 to .1.3.6.1.4.1.42.3.12.1.1.11. Each of these nodes contains an indexed list of entries with index values that range from 0 to over 27300 where the Index value represents the process ID number used by the operating system (view examples using the ps -ef command in UNIX). In this example, the index values may not be consecutive from 0 to 27300.

Community

Enter the Community string for the SNMP device. The Community string provides a level of security for a SNMP device. Most devices use "public" as a community string. However, the device you are going to monitor may require a different Community string in order to access it. You will have to find out if the device requires different string and supply it in this text box.

Advanced Settings for the SNMP Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the SNMP Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

SNMP Version (V1 or V2)

Select the SNMP version used by the SNMP host you want to monitor. SiteScope supports both SNMP version 1 and version 2.

Timeout

Enter the total number of seconds SiteScope should wait for a successful reply.

Retry Delay

Enter the number of seconds SiteScope should wait before retrying the request. By default SiteScope will wait one second. It will continue to retry at the interval specified here until the Timeout threshold is met.

Scaling

If you choose a scaling option from the scaling drop-down list, SiteScope will divide the returned value by this factor before displaying it. Alternatively, you may specify a factor by which the value should be divided in the text box to the right of the drop-down list.

Match Content

Use this item to match against an SNMP value, using a string or a regular expression or XML names.

Units

Enter an optional units string to append when displaying the value of this counter.

Measurement Label

Enter an optional text string to describe the measurement being made by the monitor.

Measure as Delta

Click this box to have SiteScope report the measurement as the difference between the current value and the previous value.

Measure as Rate per Second

Click this box to have SiteScope divide the measurement by the number of seconds since the last measurement.

Percentage Base

Enter a number or SNMP object ID in this box. If entered, the measurement will be divided by this value to calculate a percentage. If an object ID if entered the Index from above will be used

Measure Base as Delta

Check this box to have SiteScope calculate the Percentage Base as the difference between the current base and the previous base. Use this option when an SNMP object ID is used for Percentage Base and the object is not a fixed value.

SNMP V3 Username

If you are using SNMP version 3, enter the username to be used for authentication.

Note: SiteScope only supports MD5 authentication for SNMP V3.

SNMP V3 Password

If you are using SNMP version 3, enter the password to be used for authentication for SNMP V3.

Note: SiteScope only supports MD5 authentication for SNMP V3.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set up to ten status thresholds criteria for each status condition per monitor instance. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the SNMP or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the SNMP Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

62

SNMP by MIB Monitor

The SNMP by MIB Monitor allows you to monitor objects on any SNMP agent. The error and warning thresholds for the monitor can be set on one or more different objects.

This chapter describes:	On page:
About the SNMP by MIB Monitor	617
Configuring the SNMP by MIB Monitor	618
Troubleshooting MIB Compilation	626

About the SNMP by MIB Monitor

The SNMP by MIB Monitor operates like many other browsable monitors: it gathers information from a source, organizes it into a browsable tree structure, and allows the user to choose which items in the tree it should monitor. It works by connecting to the specified SNMP agent and performing a full traversal of the MIB's implemented by the agent. Thus, the user does not need to know which objects are present on the agent in advance.

The MIB files in SiteScope/templates.mib are then used to create a browsable tree that contains names and descriptions of the objects found during the traversal. Note that an object may or may not be displayed with a textual name and description, depending on the MIB's available in SiteScope/templates.mib. SiteScope does not display objects for user selection when it has no knowledge of how to display those objects. For example, a plain OctetString may contain binary or ascii data, but SiteScope has no way to decode and display this data correctly without more information.

The default run schedule for this monitor is every 10 minutes, but you can change it to run more or less often using the Frequency setting.

Configuring the SNMP by MIB Monitor

The SNMP by MIB Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the SNMP by MIB Monitor.

Main Settings for the SNMP by MIB Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the network component, how often this SNMP by MIB Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this SNMP by MIB monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the SNMP by MIB Monitor should system check the network component. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Server

Enter the name of the server you want to monitor.

MIB File

Select the MIB file which contains the objects you are interested in monitoring. If you select a specific MIB file, then only the objects described in that MIB file are displayed. If you select "All MIBs", then all objects retrieved from the agent during the MIB traversal will be displayed. If no MIB information is available for an object, it is still displayed, but with no textual name or description. To make this monitor aware of new or additional MIBs, simply place new MIB files in the SiteScope/templates.mib directory.

SNMP Version

Select the version of SNMP to use when connecting.

Community

Enter the community string (valid only for version 1 or 2 connections).

SNMP V3 Authentication Type

Select the type of authentication to use for version 3 connections.

SNMP V3 Username

Enter the username for version 3 connections.

SNMP V3 Authentication Password

Enter the authentication password to use for version 3 connections.

SNMP V3 Privacy Password

Enter the privacy password if DES privacy encryption is desired for version 3 connections. Leave blank if you do not want privacy.

SNMP V3 Context Engine ID

Enter a hexadecimal string representing the Context Engine ID to use for this connection. This is applicable for SNMP V3 only.

SNMP V3 Context Name

Enter the Context Name to use for this connection. This is applicable for SNMP V3 only.

Counters

You use the features associated with the **Counters** setting to choose and manage the metrics you want to monitor with the SNMP by MIB Monitor. Use the following steps to select and add counters.

To select or add counters:

1. Click **Get Counters** to query the remote system. After SiteScope has successfully connected to the remote system, the Get Counters selection dialogue opens.
2. Use the features in the Get Counters selection dialogue screen to select the network component metrics you want to monitor. Use the expandable menu controls as applicable to browse the available counters.
3. Use the check boxes to select between one and ten counters to be monitored.
4. Click **OK** to add the selected counters to the monitor configuration. The Get Counters selection dialogue closes and the monitor properties are updated with your selection.

Use the following steps to remove a counter from the selected counters list.

To remove or edit counters:

1. Click to edit the monitor for which you want to remove counters. Alternately, you may select the monitor you want to edit and click the Properties tab and click the **Edit** button. The monitor Properties screen opens.
2. Click the **Get Counters** button to open the Get Counters selection dialogue.
3. Clear the check box to the left of the current counter you want to remove.

At this point, you may add other counters to the monitor by clicking the applicable check boxes.

4 Click **OK** at the bottom of the screen to update the monitor.

Advanced Settings for the SNMP by MIB Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the SNMP by MIB Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Timeout

Enter the total time, in seconds, that SiteScope should wait for all SNMP requests (including retries) to complete.

Retries

Enter the number of times each SNMP GET request should be retried before SiteScope considers the request to have failed.

Port

Enter the port to use when requesting data from the SNMP agent. The default of 161 is the port on which an SNMP agent will typically be listening.

Counter Calculation Mode

Use this option to perform a calculation on objects of type Counter, Counter32, or Counter64. The available calculations are:

➤ a simple delta of the current value from the previous value, OR

➤ a rate calculation using the delta of current value from previous value, divided by the time elapsed between measurements

---

Note: This option only applies to the aforementioned object types. An SNMP by MIB Monitor that monitors Counter objects as well as DisplayString objects will only perform this calculation on the Counter objects.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set one or more status thresholds criteria for each status condition per monitor instance. The status of the monitor and any associated alert action will be set based on comparison of all the threshold criteria you define for the monitor. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the SNMP by MIB or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1 Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.

2 Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.

3 Enter a value applicable to the measurement parameter in the third text box.

4 To add another threshold setting, click the **New Error If** button and repeat the steps above.

5 Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the SNMP by MIB Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

Troubleshooting MIB Compilation

As mentioned above, you can add to the MIBs of which SiteScope is aware by putting new MIB files in the templates.mib directory. In order to recompile any new MIBs, you must restart SiteScope. Unfortunately, since MIB files may depend on other MIB files, and because ASN.1 syntax is not always obeyed completely by vendors, you may encounter compilation errors with some MIBs. Below is a series of steps you can follow when compiling new MIBs and troubleshooting compilation failures:

- Add new MIB files to the templates.mib directory. SiteScope only compiles MIBs in ASN.1 format which abide by the SMIv1 or SMIv2 standards.

- Restart SiteScope.

- Proceed as if to add a new SNMP by MIB Monitor. Before adding the monitor, check to see that your new MIB files are listed in the MIB File drop-down box. If they are, then they were successfully compiled and you may now use the SNMP by MIB monitor and the SNMP by MIB tool to browse devices that implement these MIBs. If your newly added MIBs are not listed in the MIB File drop-down box, then proceed to the next step.

- Open the file error.log in the logs directory. Look for error messages about MIB compilation near the time of your most recent restart. The error messages in this file contain descriptions of compilation errors encountered per file. The line numbers are included in these error messages, so identifying the source of the errors should not be very difficult.

- Correct the errors found in error.log. Usually, these errors can be fixed by one of the following:

- Adding a MIB to templates.mib on which some of the new MIBs depend.

- Removing a MIB from templates.mib which is duplicated or upgraded in the new MIBs.

- Fixing broken comments in the new MIBs. Note that a comment is defined as follows: "ASN.1 comments commence with a pair of adjacent hyphens and end with the next pair of adjacent hyphens or at the end of the line, whichever occurs first." This means that a line containing only the string "----" is a syntax error, whereas the a line containing only the string "----" is a valid comment. Beware of lines containing only hyphens, as adding or subtracting a single hyphen from such lines may break compilation for that MIB.

- Fixing missing IMPORT statements. Some MIBs may neglect to import objects that they reference which are defined in other MIBs.

- After correcting the errors described in error.log, restart SiteScope and follow the procedure above to verify that the new MIB files compiled correctly.

63

SNMP Trap Monitor

The SNMP Trap Monitor watches for SNMP Traps received by SiteScope from other devices. The agents for the SNMP enabled devices need to be configured to send traps to the SiteScope server.

This chapter describes:	On page:
About the SNMP Trap Monitor	629
Configuring the SNMP Trap Monitor	630

Note: To have SiteScope query a specific device for a specific value, use the SNMP Monitor.

About the SNMP Trap Monitor

The SNMP Trap Monitor is useful for automatically collecting SNMP Traps from other devices. With SiteScope doing this for you at set intervals, you can eliminate the need to check for the SNMP Traps manually. In addition, you can be notified of warning conditions that you might have otherwise been unaware of until something more serious happened. Each time that it runs this monitor, SiteScope checks traps that have been received since the last time it ran.

You will also need to configure the network devices to send SNMP Traps to SiteScope. On Windows 2000 systems, this can be configured via the Administrative Tools-->Services-->SNMP Service-->Properties-->Traps screen. SNMP agents on UNIX platforms usually require that you edit the configuration files associated with the agent. For an example of working with other devices, see the instructions on the Cisco Web site for SNMP Traps and Cisco Devices.

Note: The SNMP Trap Monitor uses port 162 for receiving traps. If another application or process on the machine where SiteScope is running has bound this port, the monitor will report an "Address in use" error and the monitor type will be unavailable.

Configuring the SNMP Trap Monitor

The SNMP Trap Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the SNMP Trap Monitor.

Main Settings for the SNMP Trap Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the infrastructure components, how often this SNMP Trap Monitor instance should be run, and the text name used for this monitor instance. See “Common Monitor Settings” in the chapter “Working with SiteScope Monitors” for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this SNMP Trap monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the SNMP Trap Monitor should system check the infrastructure components. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Content Match

Enter the text to look for in SNMP Traps. Regular expression may also be used in this box for pattern matching.

All of the SNMP Traps received by SiteScope are logged to **SiteScope/logs/SNMPTrap.log**

For example, the following shows two traps received from one router and another trap received from a second router:

```
09:08:35 09/10/2001 from=router1/10.0.0.133 oid=.1.3.6.1.4.1.11.2.17.1
trap=link down specific=0 traptime=1000134506 community=public
agent=router1/10.0.0.133 var1=The interface Serial1 is down
09:08:45 09/10/2001 from=router1/10.0.0.133 oid=.1.3.6.1.4.1.11.2.17.1
trap=link up specific=0 traptime=1000134520 community=public
agent=router1/10.0.0.133 var1=The interface Serial1 is up
09:10:55 09/10/2001 from=router2/10.0.0.134 oid=.1.3.6.1.4.1.11.2.17.1
trap=enterprise specific specific=1000 traptime=1000134652 community=public
agent=router2/10.0.0.134 var1=CPU usage is above 90%
```

Note: The three examples shown here may wrap across multiple lines to fit on this page. The actual traps may a single extended line for each trap.

Run Alert

Select the method for running alerts. If "for each event matched" is chosen, then the monitor triggers alerts for every matching entry found.

Note: When the SNMP Trap Monitor is run in the "for each event matched" alert method, the monitor will never report a status of error or warning, regardless of the results of the content match or even if the target SNMP Trap is not found.

If the "once, after all events have been checked" method is chosen, then the monitor counts up the number of matches and triggers alerts based on the **Error if** and **Warning if** thresholds defined for the monitor in the Advanced Settings section.

Advanced Settings for the SNMP Trap Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the SNMP Trap Monitor and its display in the product interface. See “Common Monitor Settings” in the chapter “Working with SiteScope Monitors” for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See “Common Monitor Settings” in the chapter “Working with SiteScope Monitors” for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set up to ten status thresholds criteria for each status condition per monitor instance. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the SNMP Trap or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the SNMP Trap Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

64

SQL Server Monitor

The SQL Server Monitor allows you to monitor the availability and performance of an Microsoft SQL Server (versions 6.5, 7.1, 2000) on Windows NT systems. The error and warning thresholds for the monitor can be set on one or more SQL Server performance statistics.

This chapter describes:	On page:
About the SQL Server Monitor	637
Configuring the SQL Server Monitor	638

About the SQL Server Monitor

Use the SQL Server Monitor to monitor the server performance metrics pages for SQL Servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate monitor instance for each SQL Server you are running.

The SQL Server Monitor makes use of Performance Counters to measure application server performance. SiteScope will need to be running under an account that has the necessary administrative security privileges to access performance counter data from remote servers. If the servers you want to monitor are in a different domain, are governed under a different policy, or require a unique login different than the account SiteScope is running under, then you will need to define the connection to these servers under the NT Remote Preferences option in the SiteScope Preferences container.

The Remote Registry service must be running on the machine where the SQL Server is running if the SQL Server is running on Windows 2000.

The default run schedule for this monitor is every 10 minutes, but you can change it to run more or less often using the **Frequency** setting.

Configuring the SQL Server Monitor

The SQL Server Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the SQL Server Monitor.

Main Settings for the SQL Server Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the SQL database server, how often this SQL Server Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this SQL Server monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the SQL Server Monitor should server check the SQL database server. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Server

Choose the server where the SQL Server you want to monitor is running. Use the drop-down list to select a server from the list of remote servers that are available to the SiteScope agent.

Counters

You use the features associated with the **Counters** setting to choose and manage the metrics you want to monitor with the SQL Server Monitor. Use the following steps to select and add counters.

To select or add counters:

1. Click **Get Counters** to query the remote system. After SiteScope has successfully connected to the remote system, the Get Counters selection dialogue opens.
2. Use the features in the Get Counters selection dialogue screen to select the SQL database server metrics you want to monitor. Use the expandable menu controls as applicable to browse the available counters.
3. Use the check boxes to select between one and ten counters to be monitored.
4. Click **OK** to add the selected counters to the monitor configuration. The Get Counters selection dialogue closes and the monitor properties are updated with your selection.

Use the following steps to remove a counter from the selected counters list.

To remove or edit counters:

1. Click to edit the monitor for which you want to remove counters. Alternately, you may select the monitor you want to edit and click the Properties tab and click the **Edit** button. The monitor Properties screen opens.
2. Click the **Get Counters** button to open the Get Counters selection dialogue.
3. Clear the check box to the left of the current counter you want to remove.

   At this point, you may add other counters to the monitor by clicking the applicable check boxes.
4. Click **OK** at the bottom of the screen to update the monitor.

Some of the performance parameters or counters available for the SQL Server Monitor include:

- % Total Processor Time (NT)
- % Processor Time (2000)
- Cache Hit Ratio
- I/O-Batch Writes
- I/O-Outstanding Reads
- I/O-Outstanding Writes
- I/O-Page Reads/sec
- I/O-Transactions/sec
- Lock Waits/sec
- Lock Wait Time (msec)
- Average Latch Wait Time (msec)
- Batch Requests/sec
- Failed Auto-Params/sec
- SQL Compilations/sec
- SQL Re-Compilations/sec
- Logins/sec
- Logouts/sec
- User Connections
- Connection Memory (KB)
- Lock Blocks
- Lock Blocks ALlocated
- Memory Grants Outstanding
- Optimizer Memory
- SQL Cache Memory
- Total Server Memory
- Cache Hit Ratio
- Cache Object Counts
- Cache Pages
- Cache Use Counts/sec

Advanced Settings for the SQL Server Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the SQL Server Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set one or more status thresholds criteria for each status condition per monitor instance. The status of the monitor and any associated alert action will be set based on comparison of all the threshold criteria you define for the monitor. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the SQL Server or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the SQL Server Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

65

SunONE Server Monitor

The SunONE Server Monitor allows you to monitor the availability of SunONE or iPlanet 6.x servers using the stats-xml performance metrics file (iwsstats.xml or nesstats.xml) facility. By providing the URL of this stats-xml file, SiteScope can parse and display all metrics reported in this file and allow you to choose those metrics you need to be monitored as counters. In addition, several derived counters are provided for your selection which measure percent utilization of certain system resources. Error and warning thresholds for the monitor can be set on one or more SunONE server performance statistics or HTTP response codes.

This chapter describes:	On page:
About the SunONE Server Monitor	645
Configuring the SunONE Server Monitor	646
SunONE Server Counters	653
Browse Counters Utility	656

About the SunONE Server Monitor

Use the SunONE Server Monitor to monitor performance metrics reported in the stats-xml file of SunONE servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate monitor instance for each SunONE server you are running.

Before you can use the SunONE Server Monitor, the "stats-xml" service option must be enabled on each Web server you want to monitor. This normally requires that you manually edit the obj.conf configuration file for each server instance. For iPlanet 6.0 servers, the entry has the following syntax:

```
<Object name="stats-xml">
ObjectType fn="force-type" type="text/xml"
Service fn="stats-xml"
</Object>
```

Each server instance must be restarted for the changes to become effective.

The default run schedule for this monitor is every 10 minutes, but you can change it to run more or less often using the **Frequency** setting.

Configuring the SunONE Server Monitor

The SunONE Server Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the SunONE Server Monitor.

Main Settings for the SunONE Server Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the SunONE server, how often this SunONE Server Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this SunONE Server monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the SunONE Server Monitor should system check the SunONE server. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Stats-XML URL

Specify the URL to the stats-xml file on the SunONE server you want to monitor. This is usually in the form http://*server_id:port*/stats-xml/*stats-xml-file*, where *stats-xml-file* is either nesstats.xml or iwsstats.xml.

HTTP Proxy

Optionally, a proxy server can be used to access the server. Enter the domain name and port of an HTTP Proxy Server.

Proxy Server User Name

If the proxy server requires a name and password to access the server, enter the name here. Your proxy server must support Proxy-Authenticate for these options to function.

Proxy Server Password

If the proxy server requires a name and password to access the server, enter the password here.

Counters

You use the features associated with the **Counters** setting to choose and manage the metrics you want to monitor with the SunONE Server Monitor. Use the following steps to select and add counters.

To select or add counters:

1. Click **Get Counters** to query the remote system. After SiteScope has successfully connected to the remote system, the Get Counters selection dialogue opens.
2. Use the features in the Get Counters selection dialogue screen to select the SunONE server metrics you want to monitor. Use the expandable menu controls as applicable to browse the available counters.

3 Use the check boxes to select between one and ten counters to be monitored.

4 Click **OK** to add the selected counters to the monitor configuration. The Get Counters selection dialogue closes and the monitor properties are updated with your selection.

Use the following steps to remove a counter from the selected counters list.

To remove or edit counters:

1 Click to edit the monitor for which you want to remove counters. Alternately, you may select the monitor you want to edit and click the Properties tab and click the **Edit** button. The monitor Properties screen opens.

2 Click the **Get Counters** button to open the Get Counters selection dialogue.

3 Clear the check box to the left of the current counter you want to remove.

At this point, you may add other counters to the monitor by clicking the applicable check boxes.

4 Click **OK** at the bottom of the screen to update the monitor.

See the section on "SunONE Server Counters" below for an explanation of the counters available for the SunONE/iPlanet 6.0 server.

Advanced Settings for the SunONE Server Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the SunONE Server Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Timeout

The number of seconds that the monitor should wait for a response from the server before timing-out. Once this time period passes, the monitor will log an error and report an error status.

Note: Depending on the activity on the server, the time to build the server monitor statistics Web page may take more than 15 seconds. You should test the monitor with an Timeout value of more than 60 seconds to allow the server time to build and serve the server monitor statistics Web page before the SiteScope monitor is scheduled to run again.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set one or more status thresholds criteria for each status condition per monitor instance. The status of the monitor and any associated alert action will be set based on comparison of all the threshold criteria you define for the monitor. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the SunONE Server or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1 Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.

2 Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.

3 Enter a value applicable to the measurement parameter in the third text box.

4 To add another threshold setting, click the **New Error If** button and repeat the steps above.

5 Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the SunONE Server Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see “Common Monitor Settings” in the chapter Chapter 2, “Working with SiteScope Monitors.”

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see “Working with Categories” in *Working with Monitor Administration*.

SunONE Server Counters

After you have specified the target SunONE server to monitor, click the **Browse** Counters button. The stats-xml file you specified will be retrieved and parsed for all metrics listed in the file, and a browse tree will be displayed. See the Browsable Counters Utility help page for instructions on how to navigate this hierarchy tree and select your counters of interest. You will notice that certain counter names listed are "qualified" with an '@' sign. The reason is that these counters can occur in multiple instances, and without qualifying them by an attribute like "id" or "pid", the multiple counter instances would be indistinguishable.

Note: At this time there is limited support for servers with multiple running processes (that is, multiple occurring <process> elements in the returned stats-xml file). Due to the dynamic nature of processes and process IDs, the scheme mentioned above cannot be used to disambiguate process elements. Therefore only the first <process> element encountered in the stats-xml file will be monitored.

Derived Counters

If you expand the *stats* node of the browse counters hierarchy, you will see a *Derived Counters* node. When you expand this node you should see a list of "virtual" counters whose values are derived from stats-xml counters. These derived counters are provided for your convenience, and are defined as follows:

Cache table utilization

This counter may help determine the efficiency of your file cache, and is defined as: the number of entries currently in the file cache divided by the maximum number of file cache entries allowed. That is, process/cache-bucket/countEntries / process/cache-bucket/maxEntries

Cache heap utilization

This counter may help determine the efficiency of your file content cache, and is defined as: the current size of the file content cache heap divided by the maximum file content cache heap size. That is, process/cache-bucket/sizeHeapCache / process/cache-bucket/maxHeapCacheSize

Percent file cache hits

This counter may help determine the efficiency of your file cache, and is defined as: the number of successful file cache lookups divided by the total number of file cache lookup attempts. That is, process/cache-bucket/countHits / (process/cache-bucket/countMisses + process/cache-bucket/countHits)

Percent idle threads

This counter may help determine the efficiency of your thread pool, and is defined as: the number of request-processing threads currently idle divided by the total number of request-processing threads that currently exist on the system. That is, process/thread-pool-bucket/countThreadsIdle / process/thread-pool-bucket/countThreads

DNS cache utilization

This counter may help determine the efficiency of your DNS cache, and is defined as: the number of entries currently in DNS cache divided by the maximum number of entries that the cache can accommodate . That is, process/dns-bucket/countCacheEntries / process/dns-bucket/maxCacheEntries

Percent DNS cache hits

This counter may help determine the efficiency of your DNS cache, and is defined as: the number of successful DNS cache lookups divided by the total number of DNS cache lookup attempts. That is, process/dns-bucket/countCacheHits / (process/dns-bucket/countCacheMisses + process/dns-bucket/countCacheHits)

Percent DNS cache misses

This counter may help determine the efficiency of your DNS cache, and is defined as: the number of unsuccessful DNS cache lookups divided by the total number of DNS cache lookup attempts. That is, process/dns-bucket/countCacheMisses / (process/dns-bucket/countCacheMisses + process/dns-bucket/countCacheHits)

Cache memory utilization

This counter may help determine the efficiency of your memory mapped file content cache, and is defined as: the amount of address space currently used by the memory mapped file content cache divided by the maximum amount of address space that the file cache uses for memory mapped file content. That is, process/cache-bucket/sizeMmapCache / process/cache-bucket/maxMmapCacheSize

Percent file info cache hits

This counter may help determine the efficiency of your file information cache, and is defined as: the number of successful file information lookups divided by the total number of file information lookup attempts. That is, process/cache-bucket/countInfoHits / (process/cache-bucket/countInfoMisses + process/cache-bucket/countInfoHits)

Percent file content cache hits

This counter may help determine the efficiency of your file content cache, and is defined as: the number of successful file content lookups divided by the total number of file content lookup attempts. That is, process/cache-bucket/countContentHits / (process/cache-bucket/countContentMisses + process/cache-bucket/countContentHits)

At this time there is no support for adding new derived counter definitions.

Browse Counters Utility

Browsing counters is a two step process. First of all, you are asked to input the "Connection Properties" which identifies which device you wish to browse along with any other information required to connect to that device.

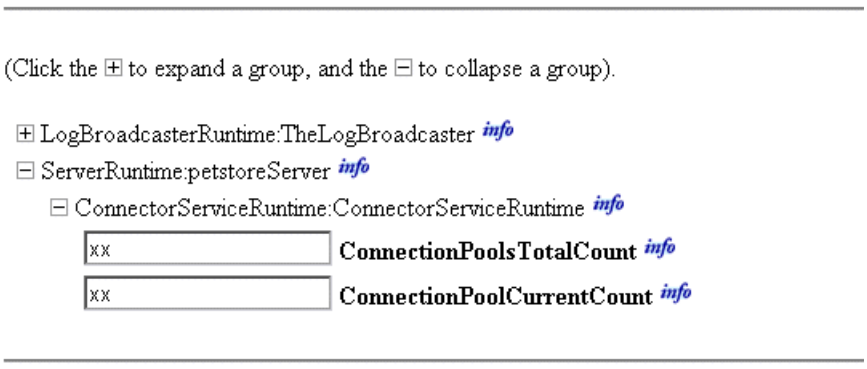
The second step is to browse and select the desired counters.

Connection Properties

The first page allows you to specify the connection properties for the device you want to browse. These properties include the device name and may include other properties such as port, username, password, and so forth, Enter the requested information and click the **Browse** button to see the available counters.

The Tree View of Counters

The Counter Tree View allows you to view the counters available for the selected device and their associated relationships. An example of a Counter Tree is shown below.



The counters are displayed in a tree structure which is initially fully collapsed. All objects will be preceded with a + or - which allows you to expand or collapse the display of that object. All counters are displayed in bold and are preceded with a check box used to indicated which counters are selected. The info graphic indicates that an explanation is available for that item. Place the cursor over the info graphic to display the information.

Expand All

Expands the entire tree to show all objects and counters. Counter selections are not affected.

Clear Selections

De-selects all counters and fully collapses the tree.

Reload Counters

Reloads the counters from the target device. Counter selections and the tree view are not affected.

Cancel

Returns to the monitor setup page without saving any connection properties or counter selections

Choose

Saves the selected counters and connection properties and returns to the monitor setup page.

Note: This information is not permanently saved until you hit **Add/Update** from the monitor setup page.

66

Sybase Monitor

The Sybase Monitor allows you to monitor the availability and performance statistics of a Sybase Server. The error and warning thresholds for the monitor can be set on one or more Sybase server performance statistics.

This chapter describes:	On page:
About the Sybase Monitor	659
Configuring the Sybase Monitor	660

About the Sybase Monitor

Use the Sybase Monitor to monitor the server performance data for Sybase database servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate monitor instance for each Sybase server in your environment.

Before you can use the Sybase Monitor you have to configure the Sybase server environment. The Sybase Monitor connects to the Sybase ASE server via the Adaptive Server Enterprise Monitor Server and retrieves metrics from the server using Sybase-provided libraries. When connecting to the monitored server, you connect to the Adaptive Server Enterprise Monitor Server, not the Sybase server. The Adaptive Server Enterprise Monitor Server is an application that runs on the same machine as Sybase server and retrieves performance information from the Sybase server. The Adaptive Server Enterprise Monitor Server usually has the same server name as the Sybase server, but with the suffix _ms. For example, if the name of the Sybase database application server is back-enddb the name of the Adaptive Server Enterprise Monitor Server for that server would be back-enddb_ms.

You also have to install the "Sybase Central" client on the machine where SiteScope is running in order to connect to the Adaptive Server Enterprise Monitor Server. The version of the client software that you install must be at least as recent or more recent than the version of the server you are trying to monitor. For example, if you have Sybase version 11.0 servers, you need to use the Sybase Central client version 11.0 or later. You will also need to know the port number used to connect to the Sybase server. You can use the dsedit tool in the Sybase client console to test connectivity with the Adaptive Server Enterprise Monitor Server.

Configuring the Sybase Monitor

The Sybase Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the Sybase Monitor.

Main Settings for the Sybase Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the Sybase database server, how often this Sybase Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this Sybase monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the Sybase Monitor should system check the Sybase database server. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Server

Choose the server where the Sybase you want to monitor is running. Use the drop-down list to select a server from the list of remote servers that are available to the SiteScope agent.

Counters

You use the features associated with the **Counters** setting to choose and manage the metrics you want to monitor with the Sybase Monitor. Use the following steps to select and add counters.

To select or add counters:

1. Click **Get Counters** to query the remote system. After SiteScope has successfully connected to the remote system, the Get Counters selection dialogue opens.
2. Use the features in the Get Counters selection dialogue screen to select the Sybase database server metrics you want to monitor. Use the expandable menu controls as applicable to browse the available counters.
3. Use the check boxes to select between one and ten counters to be monitored.
4. Click **OK** to add the selected counters to the monitor configuration. The Get Counters selection dialogue closes and the monitor properties are updated with your selection.

Use the following steps to remove a counter from the selected counters list.

To remove or edit counters:

1. Click to edit the monitor for which you want to remove counters. Alternately, you may select the monitor you want to edit and click the Properties tab and click the **Edit** button. The monitor Properties screen opens.
2. Click the **Get Counters** button to open the Get Counters selection dialogue.
3. Clear the check box to the left of the current counter you want to remove.

   At this point, you may add other counters to the monitor by clicking the applicable check boxes.
4. Click **OK** at the bottom of the screen to update the monitor.

Some of the performance objects and counters available for the Sybase Monitor include:

"**Cache**
% Hits
Pages(Read)
Pages(Read)/sec
Pages from disk(read)
Pages from disk(read)/sec
Pages write
Pages write/sec

"**Disk master**
Reads
Reads/sec
Writes
Writes/sec
Waits
Waits/sec
Grants
Grants/sec

"**Engine**
Server is busy(%)
CPU time

"Engine
Logical pages(Read)
Logical pages(Read)/sec
Pages from disk(Read)
Pages from disk(Read)/sec
Pages stored
Pages stored/sec

"Lock
% Requests
Locks count
Locks count/sec
Granted immediately
Granted immediately/sec
Granted after wait
Granted after wait/sec
Not granted
Not granted/sec
Wait time(avg)

"Memory Manager
Cache size

"**Network**
Average packet size(Read)
Average packet size(Send)
Network bytes(Read)
Network bytes(Read)/sec
Network bytes(Send)
Network bytes(Send)/sec
Network Packets(Read)
Network Packets(Read)/sec
Network Packets(Send)
Network Packets(Send)/sec

"**Process**
% Processor Time (process)
Locks/sec %
Cache Hit Pages (write)

"**SqlSrvr**
Locks/sec
% Processor Time(server)
Transactions
Deadlocks

"Stored procedures
Executed (sampling period)
Executed (session)
Avg. Duration (sampling period)
Avg. Duration (session)

"Transaction
Transactions
Transactions/sec
Rows(deleted)
Rows(deleted)/sec
Inserts
Inserts/sec
Updates
Updates/sec
Updates in place
Updates in place/sec

Advanced Settings for the Sybase Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Sybase Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule

➤ Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set one or more status thresholds criteria for each status condition per monitor instance. The status of the monitor and any associated alert action will be set based on comparison of all the threshold criteria you define for the monitor. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the Sybase or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the Sybase Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

67

Tuxedo Monitor

The Tuxedo Monitor allows you to monitor the availability of an BEA Tuxedo server. The error and warning thresholds for the monitor can be set on one or more Tuxedo Monitor performance statistics.

This chapter describes:	On page:
About the Tuxedo Monitor	671
Configuring the Tuxedo Monitor	672

About the Tuxedo Monitor

Use the Tuxedo Monitor to monitor the server performance data for BEA Tuxedo servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate monitor instance for each Tuxedo server in your environment.

Before you can use the Tuxedo Monitor, there are a number of configuration requirements involving the Tuxedo environment. An overview follows:

- If SiteScope is running as a machine in the same domain as the Tuxedo server then SiteScope can connect to the Tuxedo server as a native client. If SiteScope is outside the domain of the Tuxedo server, you will need to install, configure, and enable the Tuxedo Workstation component to allow SiteScope to make requests of the Tuxedo server.
- The client and server side workstation component software versions should be the same. Some versions of the client software can work with multiple versions of Tuxedo servers but support information is limited.

- If Tuxedo 7.1 or later is installed on both the server you want to monitor and the SiteScope server, more than one Tuxedo server can be monitored at a time. If Tuxedo 6.5 or earlier is used, only one Tuxedo server can be monitored at a time.
- If SiteScope is outside the domain of the Tuxedo server, the Tuxedo Workstation client software needs to be installed on the server where SiteScope is running. This is usually is a DLL called libwsc.dll. The address to the application server needs to be specified in the WSNADDR environment variable.
- On the server where the Tuxedo application server is running, set the TUXDIR variable to be the TUXEDO installation directory and add the TUXEDO bin directory to the PATH variable.
- The following environment variables need to be added to the SiteScope environment:
- %TUXDIR% should be set on the monitoring machine to the <Tuxedo_root_folder>
- <Tuxedo_root_folder>\bin should be added to %PATH% variable

---

Note: Any environment variables (for example, TUXDIR) should be defined as system variables, not user variables.

Configuring the Tuxedo Monitor

The Tuxedo Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the Tuxedo Monitor.

Main Settings for the Tuxedo Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the Tuxedo server, how often this Tuxedo Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this Tuxedo monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the Tuxedo Monitor should check the Tuxedo server. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Server

Enter the name or IP address of the server. The address should match that dedicated to the Tuxedo Workstation component (the WSL process). On UNIX servers, enter the full pathname of the applicable server.

Port

Enter the port number for the Tuxedo server. The port number should match the port dedicated to the Tuxedo Workstation component (the WSL process). The default port for the TUXEDO workstation listener is port 65535.

Username

Enter the Username if required to access the Tuxedo server.

Password

Enter the Password if required to access the Tuxedo server.

Client Name

Enter an optional client name for the Tuxedo server.

Connection Data

Enter any extra or optional Connection Data to be used for connecting to the Tuxedo server. In some cases this may be a hexadecimal number.

Counters

You use the features associated with the **Counters** setting to choose and manage the metrics you want to monitor with the Tuxedo Monitor. Use the following steps to select and add counters.

To select or add counters:

1. Click **Get Counters** to query the remote system. After SiteScope has successfully connected to the remote system, the Get Counters selection dialogue opens.
2. Use the features in the Get Counters selection dialogue screen to select the Tuxedo server metrics you want to monitor. Use the expandable menu controls as applicable to browse the available counters.
3. Use the check boxes to select between one and ten counters to be monitored.
4. Click **OK** to add the selected counters to the monitor configuration. The Get Counters selection dialogue closes and the monitor properties are updated with your selection.

Use the following steps to remove a counter from the selected counters list.

To remove or edit counters:

1. Click to edit the monitor for which you want to remove counters. Alternately, you may select the monitor you want to edit and click the Properties tab and click the **Edit** button. The monitor Properties screen opens.
2. Click the **Get Counters** button to open the Get Counters selection dialogue.
3. Clear the check box to the left of the current counter you want to remove.

At this point, you may add other counters to the monitor by clicking the applicable check boxes.

4 Click **OK** at the bottom of the screen to update the monitor.

The performance objects and counters available for the Tuxedo Monitor include:

Performance Object	Available Counters
Server	Requests per second Workload per second
Machine	Workload completed per second Workload initiated per second
Queue	Bytes on queue Messages on queue
Workstation Handler (WSH)	Bytes received per second Bytes sent per second Messages received per second Messages sent per second Number of queue blocks per second.
Server	Requests per second Workload per second

Advanced Settings for the Tuxedo Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Tuxedo Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set one or more status thresholds criteria for each status condition per monitor instance. The status of the monitor and any associated alert action will be set based on comparison of all the threshold criteria you define for the monitor. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the Tuxedo or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the Tuxedo Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

68

Unix Resources Monitor

The Unix Resources Monitor enables you to monitor multiple system statistics on a single Unix system. The error and warning thresholds for the monitor can be set on one or more server system statistics.

This chapter describes:	On page:
About the Unix Resources Monitor	681
Configuring the Unix Resources Monitor	682

About the Unix Resources Monitor

Use the Unix Resources Monitor to monitor the server system statistics on Unix servers. You can monitor multiple parameters or measurements with a single monitor instance. This allows you to monitor the remote server for loading, performance, and availability at a basic system level. See the list of example system measurements that can be monitored. Create a separate Unix Resources monitor instance for each Unix server in your environment.

The Unix Resources Monitor queries the list of Unix servers currently configured in the SiteScope Unix Remote Preferences container. In order to monitor a remote Unix server, you must define a Unix Remote connection profile for the server before you can add a Unix Resources Monitor for that server.

The default run schedule for this monitor is every 10 minutes, but you can change it to run more or less often using the **Frequency** setting.

Configuring the Unix Resources Monitor

The Unix Resources Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the Unix Resources Monitor.

Main Settings for the Unix Resources Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the Unix server, how often this Unix Resources Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this Unix Resources monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the Unix Resources Monitor should system check the Unix server. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Server

Choose the server you want to monitor. Use the drop-down list to select a server from the list of remote servers that are available to the SiteScope agent.

Measurements

You use the features associated with the Measurements option to choose and manage the server system measurements you want to check with the Unix Resources Monitor. A list to the right of this item displays the measurements currently selected for this monitor. Use the following steps to select and add measurements:

To select or add measurements:

1. Click the **Get Measurements** button to open the measurements selection panel.
2. Use the **Objects** drop down menu to select the system object for which you want to take measurements. The measurements selection panel is updated with the data relevant to the selected object.
3. If there is more than one instance of the type of object you have selected, use the check boxes in the **Instances** section to select the instance for which you want to take measurements.
4. Use the check boxes on the **Counters** section to select one or more measurements to monitor for the selected object and instance.
5. Click the **Add** button to add the selected measurements to the monitor configuration.
6. Repeat the steps above to add measurement counters for other objects on the remote server.

Use the following steps to remove a measurement counter from the selected measurements list.

To remove measurements:

1. Click to edit the monitor for which you want to remove measurement counters. Alternately, you may select the monitor you want to edit and click the Properties tab and click the **Edit** button. The monitor Properties screen opens.
2. Use the check boxes to the left of the current counters in the Measurements section to select which measurements you want to remove. The list is updated.

   At this point, you may add new measurements to the monitor by clicking the **Get Measurements** button and selecting the new measurement objects and counters.
3. Click the **X** button below the list to remove the measurements from the list. Click the **Ok** button at the bottom of the screen to update the monitor.

Examples of system counters or measurements available for the UNIX System Monitor are listed in the following table:

System Object	Example Instances	Example Counters
Disk Partition	hda hda1 hda2 hda5 hda6	#blocks aveq major minor rio rmerge rsect running ruse use wio wmerge wsect wuse
Disk Stats	3,0	blks_read/sec blks_written/sec read_io_ops/sec write_io_ops/sec
FileSystems	/ /dev/shm	1K-blocks Available Filesystem Use% Used
Inodes	/ /dev/shm	Filesystem IFree IUse% IUsed Inodes
Load Average	n/a	15minAvg 1minAvg 5minAvg

System Object	Example Instances	Example Counters
Memory	n/a	Active ActiveAnon ActiveCache Buffers Cached HighFree HighTotal Hugepagesize Inact_clean Inact_dirty Inact_laundry Inact_target LowFree LowTotal Mem MemFree MemShared MemTotal Swap SwapCached SwapFree SwapTotal
Network Interface	eth0 lo	ReceiveBytes TransmitBytes carrier colls compressed drop errs fifo frame multicast packets

System Object	Example Instances	Example Counters
Process	-bash /sbin/dhclient /sbin/mingetty /sbin/pam_timestamp_check /usr/X11R6/bin/X /usr/bin/ssh-agent /usr/libexec/bonobo-activation-server /usr/sbin/sshd [bdflush] [kapmd] [keventd] [khubd] [kjournald] [kscand] [ksoftirqd/0] [kswapd] [mdrecoveryd] bash crond cupsd fam gpm init klogd mdadm nautilus pam-panel-icon portmap ps rpc.statd sshd: syslogd xfs xinetd	CPU% MEMSIZE NUMBER RUNNING PID USER
Processor	Average Total cpu0	Idle System User User low

System Object	Example Instances	Example Counters
Processor Info	n/a	bogomips cache size coma_bug cpu MHz cpu family cpuid level f00f_bug fdiv_bug flags fpu fpu_exception hlt_bug model model name processor stepping vendor_id wp
System Stats	n/a	Context Switches/sec Interrupts/sec Page Ins/sec Page Outs/sec Swap Ins/sec Swap Outs/sec

System Object	Example Instances	Example Counters
TCP	n/a	ArpFilter DelayedACKLocked DelayedACKLost DelayedACKs EmbryonicRsts ListenDrops ListenOverflows PAWSActive PAWSEstab PAWSPassive PruneCalled RcvPruned SyncookiesFailed SyncookiesRecv SyncookiesSent TCPAbortFailed TCPAbortOnClose TCPAbortOnTimeout TCPDSACKOfoRecv TCPDSACKOfoSent TCPDSACKRecv TCPForwardRetrans TCPFullUndo TCPHPAcks TCPHPHits TCPHPHitsToUser TCPLoss TCPLossFailures TCPRenoRecovery TCPSackFailures TCPSackRecovery TCPSchedulerFailed TCPTimeouts TW TWKilled TWRecycled
Uptime	n/a	Uptime

Advanced Settings for the Unix Resources Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Unix Resources Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set one or more status thresholds criteria for each status condition per monitor instance. The status of the monitor and any associated alert action will be set based on comparison of all the threshold criteria you define for the monitor. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the Unix Resources or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1 Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.

2 Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.

3 Enter a value applicable to the measurement parameter in the third text box.

4 To add another threshold setting, click the **New Error If** button and repeat the steps above.

5 Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the Unix Resources Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see “Common Monitor Settings” in the chapter Chapter 2, “Working with SiteScope Monitors.”

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see “Working with Categories” in *Working with Monitor Administration*.

69

URL Monitor

The SiteScope URL Monitor is one of the most versatile and powerful Web monitoring tools available to Webmasters and system administrators.

This chapter describes:	On page:
About the URL Monitor	695
Configuring the URL Monitor	698

About the URL Monitor

The core function of the URL Monitor is to attempt to reach a specified Web page to verify that it can be retrieved, but it can also be used to do the following:

- Check secure pages using SSL, 128 bit SSL, and client certificates
- Check for specific content on the retrieved Web page
- Check the Web page for change
- Check for specific error messages
- Check the Web page for a value
- Retrieve detailed download information
- Check XML

When the URL Monitor retrieves a Web page, it retrieves the page's contents. A successful page retrieval is an indication that your Web server is functioning properly. The URL Monitor does not automatically retrieve any objects linked from the page, such as images or frames. You can, however, instruct SiteScope to retrieve the images on the page by selecting the Retrieve Images or Retrieve Frames box located in the Advanced Settings section of the Add URL Monitor Form.

In addition to retrieving specific Web pages, the URL Monitor can help you verify that CGI scripts and back-end databases are functioning properly. Just input the complete URL used to retrieve data from your database or trigger one of your CGI scripts, and the URL monitor will verify that the script generates a page and returns it to the user. For example, you can verify that your visitors are receiving a thank you page when they purchase something off of your site. The URL monitor's string matching capability even allows you to verify that the contents of the page are correct.

The SiteScope URL Monitors provide you with end-to-end verification that your Web server is running, serving pages correctly, and doing so in a timely manner. Because it tests end-to-end, it is also able to determine whether back-end databases are available, verify the content of dynamically generated pages, check for changed content, and look for specific values from a page.

What to Monitor

You can create URL monitors to watch pages that are critical to your Web site (such as your home page), pages that are generated dynamically, and pages that depend upon other applications to work correctly (such as pages that utilize a back-end database). Your goal is to monitor a sampling of every type of page you serve to check that things are working. There is no need to verify that every page of a particular type is working correctly -- one or two will do.

When you are choosing which pages to monitor, select pages with the lowest overhead. For example, if you have several pages that are generated by another application, monitor the shortest one with the fewest graphics. This will put less load on your server while still providing you with the information you need about system availability.

About Scheduling this Monitor

Each URL Monitor puts no more load on your server than someone accessing your site and retrieving a page, so in most cases you can schedule them as closely together as you want. Keep in mind that the length of time between each run of a monitor is equal to the amount of time that can elapse before you are notified of a possible problem.

A common strategy is to schedule monitors for very critical pages to run every 1 to 2 minutes, and then schedule monitors for less critical pages to run only every 10 minutes or so. Using this strategy, you will be notified immediately if a critical page goes down or if the entire Web site goes down, but you will not have an excessive number of monitors running all the time.

Status

Each time the URL Monitor runs, it returns a reading or status and writes it in the monitoring log file. It also writes in the log file the total time it takes to receive the designated document. This status value is also displayed in the SiteScope Monitor tables and is included as part of alert messages sent via e-mail.

The status reading shows the most recent result for the monitor. This status value is displayed in the URL Group table within SiteScope. It is also recorded in the SiteScope log files, e-mail alert messages, and can be transmitted as a pager alert. The possible status values are:

- OK
- unknown host name
- unable to reach server
- unable to connect to server
- timed out reading
- content match error
- document moved
- unauthorized
- forbidden
- not found

- proxy authentication required
- server error
- not implemented
- server busy

The status is logged as either good, warning, or error. A warning status or error status is returned if the current value of the monitor is a condition that you have defined as other than OK.

Configuring the URL Monitor

The URL Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the URL Monitor.

Main Settings for the URL Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the Web page or URL, how often this URL Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this URL monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the URL Monitor should URL check the Web page or URL. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

URL

Enter the URL that you want to monitor (for example, http://demo.thiscompany.com).

Note for HTTPS monitoring (secure HTTP): If the URL starts with HTTPS, then a secure connection will be made using SSL (for example, https://www.thiscompany.com). SiteScope uses Java SSL libraries for HTTPS monitoring.

Match Content

Enter a string of text to check for in the returned page or frameset. If the text is not contained in the page, the monitor will display "no match on content". The search is case sensitive. Remember that HTML tags are part of a text document, so include the HTML tags if they are part of the text you are searching for (for example, "< B> Hello< /B> World"). This works for XML pages as well. You may also perform a regular expression match by enclosing the string in forward slashes, with an "i" after the trailing slash indicating case-insensitive matching. (for example, "/href=Doc\d+\.html/" or "/href=doc\d+\.html/i"). If you want a particular piece of text to be saved and displayed as part of the status, use parentheses in a Perl regular expression. For example /Temperature: (\d+). This would return the temperature as it appears on the page and this could be used when setting an Error if or Warning if threshold.

Advanced Settings for the URL Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the URL Monitor and its display in the product interface. See “Common Monitor Settings” in the chapter “Working with SiteScope Monitors” for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Timeout

The number of seconds that the URL monitor should wait for a page to complete downloading before timing-out. Once this time period passes, the URL monitor will log an error and report an error status. If you have checked the Retrieve Frames or Retrieve Images option, SiteScope will wait for these items to be retrieved before considering the page to be fully downloaded.

HTTP Proxy

Optionally, a proxy server can be used to access the URL. Enter the domain name and port of an HTTP Proxy Server.

Retrieve Images

Check this box if you want the status and response time statistics to include the retrieval times for all of the embedded images in the page. Embedded images include those referenced by "IMG" and "INPUT TYPE=IMAGE" HTML tags. Images that appear more than once in a page are only retrieved once.

Note: If the Retrieve Images option is checked, each image referenced by the target URL will contribute to the download time. However, if a image times out during the download process or has a problem during the download, that time will not be added to the total download time.

Retrieve Frames

Check this box if you want SiteScope to retrieve the all frames references in a frameset and count their retrieval time in the total time to download this page. If Retrieve Images is also checked, SiteScope will attempt to retrieve all images in all frames.

Note: If the Retrieve Frames option is checked, each frame referenced by the target URL will contribute to the download time. However, if a frame times out during the download process or has a problem during the download, that time will not be added to the total download time.

Error If Match

Enter a string of text to check for in the returned page or frameset. If the text **is** contained in the page, the monitor will indicate an error condition. The search is case sensitive. Remember that HTML tags are part of a text document, so include the HTML tags if they are part of the text you are searching for (for example, "< B> Error < /B> Message"). You may also perform a regular expression match by enclosing the string in forward slashes, with an "i" after the trailing slash indicating case-insensitive matching. (for example, "/href=Doc\d+\.html/" or "/href=doc\d+\.html/i").

Check for Content Changes

Unless this is set to "no content checking" (the default) SiteScope will record a checksum of the document the first time the monitor runs and then does a checksum comparison each subsequent time it runs. If the checksum changes, the monitor will have a status of "content changed error" and go into error. If you want to check for content changes, you will usually want to use "compare to saved contents".

The options for this setting are:

- **no content checking** - (default) SiteScope does not check for content changes
- **compare to last contents** - The new checksum will be recorded as the default after the initial error "content changed error" occurs, so the monitor will return to OK until the checksum changes again
- **compare to saved contents** - The checksum is a snapshot of a given page (retrieved either during the initial or a specific run of the monitor). If the contents change, the monitor will get a "content changed error" and will stay in error until the contents return to the original contents, or the snapshot is update by resetting the saved contents

➤ **reset saved contents** - Takes a new snapshot of the page and saves the resulting checksum on the first monitor run after this option is chosen. After taking the snapshot, the monitor will revert to "compare to saved contents" mode.

Baseline Interval

Enter the number of monitor runs to be averaged for use as a Rolling Baseline. Rolling baselines are calculated for an interval equal to time to complete the number of monitor runs entered here. See more information.

HTTP Version

Check this box to force SiteScope to use HTTP version 1.0 style request headers. When unselected, SiteScope will use HTTP Version 1.1 in the request header to the target server. HTTP 1.1 is the default setting.

Retries

Enter the number of times that SiteScope should retry the request if a recoverable error was encountered. If monitor times out, the number of retries are reduced.

Accept Untrusted Certs for HTTPS

Check this option if you need to use certificates that are untrusted in the cert chain in order to access the target URL using Secure HTTP (HTTPS).

Accept Invalid Certs for HTTPS

Check this option if you need to accept an invalid certificate in order to access the target URL using Secure HTTP (HTTPS). This may happen, for example, if the current date is not in the date ranges specified in the certificate chain.

Client Side Cert

If you need to use a client side certificate to access the target URL, select the certificate file using the drop down menu. Client side certificate files must be copied into the SiteScope/templates.certificates directory. Normally, this will be a .pfx (.p12) type certificate, which usually requires a password. You enter the password for the certificate in the **Client Side Cert Password** field.

Client Side Cert Password

If you are using a client side certificate and that certificate requires a password, enter the password in this field.

Authorization User Name

If the URL specified requires a name and password for access, enter the user name in this box. Alternately, you can leave this entry blank and enter the user name in the Default Authentication Credentials section on the General Preferences page. You use this alternate method to define common authentication credentials for use with multiple Web Service monitor.

Authorization Password

If the URL specified requires a name and password for access, enter the password in this box. Alternately, you can leave this entry blank and enter the password in the Default Authentication Credentials section on the General Preferences page. You use this alternate method to define common authentication credentials for use with multiple Web Service monitor.

Authorization NTLM Domain

Enter the domain for NT LAN Manager (NTLM) authorization if it is required in order to access the URL.

Preemptive Authorization

Select when the Authorization User Name and Authorization Password should be sent as part of the URL transaction. The table below describes the options available. By default the setting specified in the Default Authentication Credentials section of the General Preferences page will be used, if they have been specified.

Note: You do not use this setting to control IF the user name and password given for this monitor instance should be sent or WHICH username and password should be sent. You use this setting to select WHEN a username and password should be sent when SiteScope requests the target URL.

Option	Description
Use Global Preference	Select this option to have SiteScope use the **When to Authenticate** setting as specified in the Default Authentication Credentials section of the General Preferences page. **Note:** This only determines when the authorization information is sent. This option will still use the **Authorization User Name** and **Authorization Password** entered for this monitor instance. If these are not specified for the individual monitor, the **Username** and **Password** specified in the Default Authentication Credentials section of the General Preferences page will be used, if they have been specified.
Authenticate first request	Select this option to send the username and password on the first request SiteScope makes for the target URL. This will use the **Authorization User Name** and **Authorization Password** entered for this monitor instance. If these are not specified for the individual monitor, the **Username** and **Password** specified in the Default Authentication Credentials section of the General Preferences page will be used, if they have been specified. **Note:** If the URL does not require a username and password, then this option may cause the URL to fail.
Authenticate if requested	Select this option to send the username and password on the second request if the server requests a username and password. This will use the **Authorization User Name** and **Authorization Password** entered for this monitor instance. If these are not specified for the individual monitor, the **Username** and **Password** specified in the Default Authentication Credentials section of the General Preferences page will be used, if they have been specified. **Note:** If the URL does not require a username and password, then this option may be used.

Proxy Server User Name

If the proxy server requires a name and password to access the URL, enter the name here. Technical note: your proxy server must support Proxy-Authenticate for these options to function.

Proxy Server Password

If the proxy server requires a name and password to access the URL, enter the password here. Technical note: your proxy server must support Proxy-Authenticate for these options to function.

POST Data

If the URL is for a POST request, enter the post variables, one per line as name=value pairs. This option is used to verify that a form is working correctly by performing the same request that occurs when a user submits a form. See also the Match Content item for a way to verify that the correct form response was received. If this item is blank, a GET request is performed.

Advanced Option The POST Data can be used to send cookie data. To send cookies with the request use the format "**Set-cookie: cookieName=cookieValue**".

To change the content type of a post, use the format "Content-Type: application/my-format". To hide values in the POST data, add a line like:

```
_private=_name=mysecret _value=rosebud
_private=_name=mypassword _privateValue=sesame
```

and then use the following form in the POST Data

```
s|username=$private-mysecret$|
s|password=$private-mypassword$|
```

and SiteScope will substitute the values from the master.config into the POST Data.

URL Content Encoding

If the URL content requested uses an encoding that is different than the encoding used on server where SiteScope is running, enter the code page or encoding to use for this step. Some examples of commonly used encodings are: Cp1252, Cp1251, Cp1256, Shift_JIS or EUC_JP. This may be necessary if the default code page which SiteScope is using does not support the character sets used in the target URL. This will enable SiteScope to match and display the encoded content correctly.

Error If Redirected

Check this box if you want SiteScope to notify you if a URL is redirected. Normally, SiteScope follows redirects without reporting an error.

Show Detailed Measurement

Check this box if you want SiteScope to record a detailed break down of the process times involved in retrieving the requested URL. This includes DNS lookup, connect time, HTTP server response time, described as follows:

- **DNS time** - The time it takes to send a name resolution request to your DNS server until you get a reply.
- **Connection time** - The time it takes to establish a TCP/IP/Socket connection to the Web server.
- **Response time** - The time after the request is sent until the first byte (rather first buffer full) of the page comes back.
- **Download time** - The time it takes to download the entire page.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting URL Monitor Status Thresholds

SiteScope URL monitor types allow you to set threshold conditions based on part or all of a Web page retrieval or transaction to determine the status reported by each monitor. Monitor status can be set based on the roundtrip, DNS, connect, or response times needed to negotiate a Web request or transaction.

The roundtrip time is one of the most commonly used metrics for URL monitoring. Roundtrip time includes the time to complete the following:

1. Name lookup (DNS)
2. Connect to the server socket
3. Send the HTTP request
4. Download the entire page

If the server hosting SiteScope is heavily loaded, either with other applications or with a high SiteScope monitoring load, then it can contribute to slower times, especially for HTTPS URLs, which are more CPU intensive. Usually though, the time waiting for the network is a much greater factor than the CPU usage.

Set the monitor status thresholds for the URL Monitor as described below.

Error if

By default, SiteScope generates an error if the returned HTTP status is anything other than 200 ("OK"), which indicates a successful retrieval. You can choose to have SiteScope report an error status based on any of the following measurements:

- round trip time - the total time for the entire request, in milliseconds
- DNS time - the amount of time to translate the host name to an IP address, in milliseconds
- connect time - the amount of time to make the connection, in milliseconds
- response time - the amount of time before the first response was received, in milliseconds
- download time - the amount of time to receive the page contents, in milliseconds
- age -- the amount of time between the current time and the last-modified time for the page, in seconds
- content match
- total errors
- overall status

Choose a comparison operator from the drop-down list, and enter a value for the comparison in the text box.

The URL Monitor follows HTTP redirect codes (301 and 302) to retrieve the actual page before returning the status of the URL retrieval. SiteScope will show a redirect error only if the redirects are more than 10 levels deep - this prevents infinite redirects from being followed, or if the Error On Redirect check box is selected.

Warning if

By default, SiteScope generates a warning if Check Images or Check Frames is chosen and there was a problem retrieving one of the images or frames. You may choose to have the monitor report a warning status based on any of the measurement options listed under Error if. Choose a comparison operator, and enter a value for the comparison to generate a warning.

Good if

By default, SiteScope reports an OK status if the URL returns an HTTP status of 200 ("OK"). You may also choose to have SiteScope base an OK status on any of the measurement options listed under Error if. Enter the value that should generate an OK status.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the URL Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

70

URL Content Monitor

The URL Content Monitor is a specialized variation of the URL Monitor that can match up to ten different values from the content of a specified URL. The matched values are displayed with the status of the monitor in the monitor group table and written to the monitor log.

This chapter describes:	On page:
About the URL Content Monitor	713
Configuring the URL Content Monitor	715

About the URL Content Monitor

The URL Content Monitor is primarily used to monitor Web pages that are generated dynamically and display statistics about custom applications. By monitoring these pages, these statistics can be retrieved and integrated into the rest of your SiteScope system.

What to Monitor

You should use the URL Content Monitor if you need to verify multiple values (up to 10 variables) from the content of a single URL. Otherwise, the standard URL Monitor is normally used. One use for this monitor is to integrate SiteScope with other applications that export numeric data through a Web page. The content values are matched using regular expressions. The monitor includes the matched values as part of the monitor status which are written to the log. If the matched values are numeric data, the results can be plotted in a report.

About Scheduling this Monitor

The frequency will depend on the statistics being monitored. For more statistics, every several minutes is often enough.

Status

Each time the URL Content Monitor runs, it returns a status and several match values and writes them in the monitoring log file. It also writes the total time it takes to receive the designated document in the log file.

The reading is the current value of the monitor. Possible values are:

- OK
- unknown host name
- unable to reach server
- unable to connect to server
- timed out reading
- content match error
- document moved
- unauthorized
- forbidden
- not found
- proxy authentication required
- server error
- not implemented
- server busy

The status is returned as good, warning, or error dependent on the results of the retrieval, content match, and the error or warning status criteria that you select.

Configuring the URL Content Monitor

The URL Content Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the URL Content Monitor.

Main Settings for the URL Content Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the Web page, how often this URL Content Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this URL Content monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the URL Content Monitor should content check the Web page. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

URL

Enter the URL that you want to monitor (for example, http://demo.thiscompany.com). If you are monitoring a secure URL, be sure the URL reflects the correct transfer protocol (for example https://demo.thiscompany.com).

Match Content

Enter an expression describing the values to match in the returned page. If the expression is not contained in the page, the monitor will display "no match on content". A regular expression is used to define the values to match. For example, the expression /Copyright (\d*)-(\d*)/ would match two values, 1996 and 1998, from a page that contained the string Copyright 1996-1998.

Advanced Settings for the URL Content Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the URL Content Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Timeout

The number of seconds that the URL monitor should wait for a page to begin downloading before timing-out. Once this time period passes, the URL monitor will log an error and report an error status.

HTTP Proxy

Optionally, a proxy server can be used to access the URL. Enter the domain name and port of an HTTP Proxy Server.

Retrieve Images

Check this box if you want the status and response time statistics to include the retrieval times for all of the embedded images in the page. Embedded images include those referenced by "IMG" and "INPUT TYPE=IMAGE" HTML tags. Images that appear more than once in a page are only retrieved once.

Note: If the Retrieve Images option is checked, each image referenced by the target URL will contribute to the download time. However, if a image times out during the download process or has a problem during the download, that time will not be added to the total download time.

Retrieve Frames

Check this box if you want SiteScope to retrieve the all frames references in a frameset and count their retrieval time in the total time to download this page. If Retrieve Images is also checked, SiteScope will attempt to retrieve all images in all frames.

Note: If the Retrieve Frames option is checked, each frame referenced by the target URL will contribute to the download time. However, if a frame times out during the download process or has a problem during the download, that time will not be added to the total download time.

Error If Match

Enter a string of text to check for in the returned page. If the text **is** contained in the page, the monitor will display "no match on content". The search is case sensitive. Remember that HTML tags are part of a text document, so include the HTML tags if they are part of the text you are searching for (for example, "< B> Error < /B> Message"). You may also perform a regular expression match by enclosing the string in forward slashes, with an "i" after the trailing slash indicating case-insensitive matching. (for example, "/href=Doc\d+\.html/" or "/href=doc\d+\.html/i").

Check for Content Changes

Check this box if you want SiteScope to notify you if the contents of this document are changed. SiteScope records a checksum of the document the first time the monitor runs and then does a checksum each subsequent time it runs. If the checksum changes, you will be notified. The new checksum will be recorded as the default after the initial error has been issued.

Authorization User Name

If the URL specified requires a name and password for access, enter the name in this box.

Authorization Password

If the URL specified requires a name and password for access, enter the password in this box.

NT Challenge Response

Check this box if you want SiteScope to use Window's NT Challenge Response authorization when retrieving this Web page.

Proxy Server User Name

If the proxy server requires a name and password to access the URL, enter the name here. Technical note: your proxy server must support Proxy-Authenticate for these options to function.

Proxy Server Password

If the proxy server requires a name and password to access the URL, enter the password here. Technical note: your proxy server must support Proxy-Authenticate for these options to function.

POST Data

If the URL is for a POST request, enter the post variables, one per line as name=value pairs. This option is used to verify that a form is working correctly by performing the same request that occurs when a user submits a form. See also the Match Content box for a way to verify that the correct form response was received. If this item is blank, a GET request is performed. Advanced: This item can also be used to pass cookies with the request. For example, "Set-cookie: cookieName=cookieValue".

Error If Redirected

Check this box if you want SiteScope to notify you if a URL is redirected. Normally, SiteScope follows redirects without reporting an error.

Show Detailed Measurement

Check this box if you want SiteScope to record a detailed break down of the process times involved in retrieving the requested URL. This includes DNS lookup, connect time, HTTP server response time, described as follows:

- **DNS time** - The time it takes to send a name resolution request to your DNS server until you get a reply.
- **Connection time** - The time it takes to establish a TCP/IP/Socket connection to the Web server.
- **Response time** - The time after the request is sent until the first byte (rather first buffer full) of the page comes back.
- **Download time** - The time it takes to download the entire page.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

Set the monitor status thresholds for the monitor as described below.

Error if

By default, SiteScope generates an error if the returned status is anything other than 200, which indicates a successful retrieval. You may choose to have SiteScope generate an error based on any of the following:

- tenth content match
- content match
- age
- second content match
- third content match
- fourth content match
- fifth content match
- sixth content match
- seventh content match
- eighth content match
- ninth content match

- download time
- connect time
- response time
- size
- dns time
- round trip time

At present, content match values used for error or warning generation must be numeric.

The URL Content Monitor follows redirect codes (301 and 302) to retrieve the actual page before returning the status of the URL retrieval. SiteScope will show a redirect error only if the redirects are more than 10 levels deep - this prevents infinite redirects from being followed, or if the Error On Redirect check box is selected.

Warning if

By default, SiteScope does not generate warnings for URL Content monitors. You may choose to generate a warning based any of the options listed under *Error if*. Enter the lowest value that should generate a warning.

Good if

By default, SiteScope returns an OK status if a 200 status is returned, but you may choose to base an ok status on any of the options listed under *Error if*. Enter the value that SiteScope should consider to be a good response.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the URL Content Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

71

URL List Monitor

The URL List Monitor is used to check a large list of URLs. This monitor is commonly used by Web hosting providers to measure the availability and performance of their customer's Web sites.

This chapter describes:	On page:
About the URL List Monitor	725
Configuring the URL List Monitor	727

About the URL List Monitor

You can use the URL List Monitor to check a list of URLs without having to create a separate URL monitor for each one. For example, this is useful if you host several Web sites and simply want to see that they are each serving pages as expected. The URL List Monitor is not used to confirm links between pages (see the Link Check Monitor) or other Web transaction processes (see the URL Sequence Monitor).

A URL List is specified by giving a filename containing the list of URLs to check. The URLs that you want to monitor are saved in a plain text file. There is virtually no limit to the number that you can list though the run interval selected for the monitor may require that the number of URLs be limited. For each URL included in the URL list file, the monitor retrieves the contents of the URL or the server response to the request.

What to Monitor

The URL List Monitor is useful for monitoring any set of URLs that you simply want to make sure are available over the network.

About Scheduling this Monitor

This is strictly dependent upon how often to want to check to see if the URLs are working. Once an hour is common, but you can schedule it to run more often.

There are a few factors that affect how long it takes the URL List Monitor to complete a run:

- number of URLs in the list
- URL retrieval time
- the number of threads used

In some cases this may lead to the monitor not running as expected. As an example, assume you have a list of 200 URLs that you want to monitor every 10 minutes, but, due to Internet traffic, SiteScope is not able to complete checking all of the 200 URLs in that amount of time. The next time the monitor was scheduled to run, SiteScope would see that it did not complete the previous run and would wait for another 10 minutes before trying again.

If this happens once in awhile, it is probably not a problem, but if it happens more often there are three things you can do to resolve the issue.

1. The most obvious option is to schedule the monitor to run less frequently, but if that conflicts with some other objective, go to options 2 and 3.
2. The second thing you can do is reduce the pause interval set under the Advanced Settings. This will minimize the time it takes for the monitor to retrieve all of the URLs.
3. The third option (which you can use in conjunction with number 2) is to increase the number of threads that SiteScope can use when checking the URLs. The more threads, the quicker SiteScope can check them. Of course, this will put a heavier load on your system, so you have to find a happy medium.

   Ideally, you want SiteScope to have just completed checking the URLs in the list when it is time to start checking again. This would indicate that the load was evenly balanced. It may take some tweaking to get it just right

Each time the URL List Monitor runs, it returns the number of errors, if any, and writes it into the monitoring log file. It also writes the total number of URLs checked and the average time, in milliseconds, to retrieve each URL.

Configuring the URL List Monitor

The URL List Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the URL List Monitor.

Main Settings for the URL List Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the URL's, how often this URL List Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this URL List monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the URL List Monitor should URL check the URL's. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

URL List Name

Enter the path name for the file containing the list of URLs to be monitored. This file should be a plain text file and contain only one URL per line of text as shown here:

```
http://www.website.com/index.html
http://www.website.com/main/customer/order.html
```

http://www.website.net/default.htm
http://www.Web pages.com/tech/support/ws/intro.html

Advanced Settings for the URL List Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the URL List Monitor and its display in the product interface. See “Common Monitor Settings” in the chapter “Working with SiteScope Monitors” for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Server

Enter the optional Server name to specify which URLs to check in the URL list. If the URLs are stored in a "map" format, this item is used to check a subset of the URLs from the list. By default, all the URLs in the list are checked.

Log

Enter the path name for the log file for this monitor. For each URL checked, an entry will be added to this log file. If this item is blank, a log is not created.

Error Log

Enter the path name for the error log file for this monitor. For each error retrieving a URL, an entry will be added to this log file. If this item is blank, a log is not created.

Threads

Enter the number of threads to retrieve URLs. This is the number of simultaneous checks to perform. Increasing this number will shorten the time for all of the URLs to be checked but also increase the load on the server.

Pause

Enter the pause, in milliseconds, between each URL check. Decreasing this number will shorten the total time required to check all of the URLs but will also increase the load on the server.

Retries

Enter the number of times you want SiteScope to try to reach URLs that are returning an error.

HTTP Proxy

Optionally, a proxy server can be used to access the URLs in the list. Enter the domain name and port of an HTTP Proxy Server.

Authorization User Name

If the URLs in the list require a name and password for access, enter the name in this box.

Authorization Password

If the URLs in the list require a name and password for access, enter the password in this box.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set up to ten status thresholds criteria for each status condition per monitor instance. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the URL List or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the URL List Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

72

URL Sequence Monitor

The SiteScope URL Sequence Monitor simulates a user's actions across a series of Web pages and URLs. This is particularly useful for monitoring and testing multi-page e-commerce transactions and other interactive online applications.

This chapter describes:	On page:
Understanding the URL Sequence Monitor	735
Working with the URL Sequence Monitor	736
Configuring the URL Sequence Monitor	738
Configuring URL Sequence Steps	739
Settings for URL Sequence Steps	746
URL Sequence Monitor Settings	750
Retaining and Passing Values Between Sequence Steps	759

Understanding the URL Sequence Monitor

You use URL Sequence Monitors to verify that multiple-page Web transactions are working properly. This is an important part of monitoring key business processes and services. For example, you can have SiteScope retrieve a login page, enter an account name via a secure Web form, check an account status for the page that is returned, and then follow a sequence of links through several more pages. URL Sequence Monitors are also useful for checking pages that include dynamically generated information, such as session IDs, that are embedded in the Web pages via dynamic links or hidden input items.

A URL Sequence begins with a URL acting as the starting point or Step 1 for the sequence. This can then be followed by additional URLs that are accessed manually, or more commonly, by links or form buttons that a user would select in order to navigate or complete a specific transaction.

By default, SiteScope allows you to define up to twenty sequence steps. For each step you may specify a content match to search for, enter a user name and password if required, define custom POST data, as well as other optional criteria for that step.

What to Monitor

You should monitor any multi-step Web page sequence that you have made available to general users to verify that they are available and function correctly. Web site visitors often assume that any problems they encounter are due to user error rather than system error, especially if they're not familiar with your application. By using this monitor to perform sequence testing, you will know that users are able to successfully complete transactions.

Working with the URL Sequence Monitor

The URL Sequence Monitor is more complex than most other SiteScope monitor types and the steps for working with the monitor are different than for other monitors. The following is an overview of key concepts and actions you use when working with the URL Sequence Monitor:

- The URL Sequence Monitor can be configured with between one to twenty steps. Each step is defined individually in a sequence of numbered entries in the interface. The steps must be initially configured in the intended sequence as the request for one step provides the content used in the following step.
- You use the **Add Step** button to add a new step to the URL sequence. You only use the **Ok** button at the bottom of the monitor properties panel after you have added all the desired steps and then you are ready to activate the monitor instance.
- When you first configure a URL Sequence Monitor, be sure to configure the steps you want to include in the sequence before you click the **Ok**

button to create the monitor. SiteScope uses a special setup process for when the monitor is first being configured. After the monitor has been added, editing the monitor to add more steps is more difficult.

- You configure the URL Sequence Monitor in text mode. The navigation links and form actions are displayed as text parsed from the HTML that is used to construct a page in Web browsers. In some cases, portions of HTML code may also be included. You need to be familiar with HTML when working with this monitor.
- Many Web-based systems use session data to identify clients and track the state of a user's interaction with the server application. This session data is often sent back and forth to the client in the HTTP header or Post Data. You should be familiar with the session tracking methods used by the systems you want to monitor in order to effectively configure this monitor.
- Web-based sequences or transactions can be difficult to navigate when dealing with many Web pages. For example, Web pages that use many graphic images for navigation hyperlinks can present special challenges when configuring URL Sequence monitors. You need to be familiar with HTML hyperlink syntax when working with this monitor.
- The Main Settings and Advanced Settings for the URL Sequence Monitor apply to the monitor in general and behave much the same as for other monitor types.
- When you first configure the URL Sequence Monitor, the HTML text content returned from the request made in one step is displayed in a folding panel a the bottom of the following Step panel. This can be very useful for finding content on which you want to perform a match. You may also use this to correlate links and forms in the respective selection menus with their relative location on the page. For example, if there is a search entry form near the top of a Web page and another, different search form further down in the page, you can view the raw HTML to help determine the syntax associated with the form that you want to test.
- SiteScope does not parse or interpret embedded scripts or other client-side program code such as Javascript (ECMAscript). Web page content that is generated or controlled by client-side code will usually not appear in the URL Sequence Wizard. See the URL Sequences and Client-side

Programs help page for more information on dealing with Web page scripts.

Configuring the URL Sequence Monitor

The URL Sequence Monitor can be added to any SiteScope monitor group container in the monitor tree. The following are the steps you use to add an URL Sequence Monitor.

To add an URL Sequence Monitor:

1. Click on the monitor group container where you want to add the URL Sequence Monitor instance.
2. In the Group Contents pane, click the **New Monitor** button. Alternately, you may right-click the group container in the left menu and select **New Monitor** from the Action Menu. The New Monitor selection pane opens.
3. Click the URL Sequence Monitor link. The New Monitor pane for the URL Sequence Monitor opens.
4. Complete the Main Settings section by entering a **Name** for the monitor instance and selecting a **Frequency**. See the section "Main Settings for the URL Sequence Monitor" for more information.
5. Configure the individual steps for the URL sequence. You do this by using the **Add Step** button in the Main Settings section. See the section "Configuring URL Sequence Steps" for more information.
6. Configure the Advanced Settings as necessary. See the section for more "Advanced Settings for the URL Sequence Monitor" information.
7. Configure the Threshold Settings for the monitor. The thresholds can be set for individual steps or for the whole monitor.
8. Click **OK** to create the new monitor instance.

   Once you have added an URL Sequence Monitor, you can edit the monitor configuration settings using the same steps as with other monitors.

Configuring URL Sequence Steps

The core of the URL Sequence Monitor is the sequence of URL and associated action requests that will be performed by the monitor. The following sections describe the steps and settings you use to create an URL sequence.

Starting a New URL Sequence

The URL sequence must begin with an initial URL. You configure the first URL in the sequence in the URL Sequence panel.

To start a new URL Sequence:

1. In the Main Settings panel of the New URL Sequence Monitor properties tab, click the **Add Step** button. The URL Sequence step dialog page opens.
2. Enter the initial URL address in **Reference Type** field. This URL should be the initial Web page that the user is expected to see or the access point for the web-based system you are going to monitor.
3. Complete the other settings as necessary. Generally, the URL will be sufficient for the first step of most URL sequences. See the section "Settings for URL Sequence Steps" for more information.
4. Click the **Ok** button at the bottom of the dialog screen to add the step.

   SiteScope will make a request for the URL entered for the **Reference Type** URL. The data returned by this initial request will be used for subsequent steps. The HTTP response header and the content of the URL will be available in a folding panel labeled HTML Source at the bottom of the subsequent step dialog box.

Defining Additional Sequence Steps

When you have entered the first step, you are ready to add more steps. You repeat this process depending on the number of Web pages and actions that need to be taken to complete the sequence. The step screens provide access to the available elements on the Web page requested by the previous step. This includes form buttons, hyperlinks, form input elements, and other data. You will use these elements to create each subsequent sequence step separately. Most sequence steps involve one of the following elements:

- Go to URL Manually
- Following a Hyperlink
- Selecting a Form Button
- Selecting a Frame within a Frameset
- Following a META REFRESH Redirection

Note: SiteScope does not parse or interpret embedded scripts or other client-side program code such as Javascript (ECMAscript). Web page content that is generated or controlled by client-side code will usually not appear in the URL Sequence Wizard.

Tools for Viewing Sequence Steps and Content

The buttons at the bottom of the step dialog page provide you with some additional tools useful for working with URL sequences. Next to the **OK** and **Cancel** buttons are two buttons you use as described below:

- **Show Source** - Click this button to open a new browser window that displays the source code of the URL returned by the previous request. You can use this window to copy data, such as a session ID or form data, from the Web page for use in the current step. The HTML Source folding panel at the bottom of the step page can also be used to view the source of the Web page. However, some browsers do not support copying data from this panel.
- **Show Page** - Click this button to open a new browser window that displays the URL in a regular browser view. You can use this window to match the **Link** and **Form** data displayed in the URL Sequence Monitor step dialog form with the elements as displayed on the Web page.

Go to URL Manually

Where the sequence uses the Common Gateway Interface (CGI) for data transmission between the client and the server, it may be useful to specify a particular URL and name-value pairs. You can enter the URL you want to request along with any name-value pairs needed to get to the next sequence step even if those values are available through some other page element (such as a form). This option also allows you to copy URL and CGI strings directly from the location or address bar of another browser client that you may be using to step through the sequence you are building.

Complete the following steps if you want to direct SiteScope to go to a URL other than those listed in the Links list.

To request a specific URL manually:

1. For the **Reference Type** option, click the radio button to the left of the **URL** text entry box.
2. Type the URL you want SiteScope to go to in the URL text entry box.
3. Complete the other step settings as necessary. Include any CGI Post or Get data that may be required. See the section "Settings for URL Sequence Steps" for more information.
4. Click the **Ok** button to add the step.
5. Use the steps in this section to add additional sequence steps. After you have added all the steps to the URL sequence, you must click the **OK** button at the bottom of the properties screen to add the monitor to SiteScope.

Following a Hyperlink

SiteScope parses the content of the URL returned by the previous step and creates a list of hyperlinks that are found on the page. This includes links that are part of an image map that may be virtual "buttons" on a navigation menu. Any links found on this page of the sequence can be viewed and selected using the drop-down list box to the right of the **Link** radio button. Use the following steps to add a link step to the sequence.

To request a URL by following a hyperlink

1. For the **Reference Type** option, click the radio button to the left of the **Link** item.

2 Click to expand the drop-down menu to display all available links on the current page. Click the label or HTML text corresponding to the hyperlink that you want SiteScope to follow. If you know a link is available on the subject page but it does not appear in the drop-down list, it may that the page uses a client-side program. In this case, you may have to specify the URL manually.

3 Complete the other step settings as necessary. See the section "Settings for URL Sequence Steps" on page 746 for more information.

4 Click the **Ok** button to add the step.

5 Use the steps in this section to add additional sequence steps. After you have added all the steps to the URL sequence, you must click the **OK** button at the bottom of the properties screen to add the monitor to SiteScope.

Selecting a Form Button

SiteScope parses the content of the URL in the current step and creates a list of form elements of the type "Submit". If SiteScope finds any HTML forms on the current page of the sequence, they will be displayed in a drop-down list.

The listings are in the following format:{[formNumber]FormName}ButtonName

For example, the *Search* button on a company's search page might be listed as:{[1]http://www.CompanyName.com/bin/search}search

To submit Form data or request:

1 For the **Reference Type** option, click the radio selection button to the left of the Form item. The drop-down list to the right of the Form item lists the form Submit button(s) found on the current page.

2 Click to expand the drop-down menu to display the list of available form buttons. Click the name or HTML text corresponding to the form button that you want SiteScope to use. If you know a form is available on the subject page but it does not appear in the drop-down list, see the note below about client-side programs.

3 Below the list of form submit buttons is the Post Data field that contains a listing of form input items available for this page. Locate the one(s) that pertain to the form associated with the submit button you selected and type

the appropriate data in to the Post Data text box. Note that there may be more than one form on the page.

Post Data is submitted as name-value pairs. Enter the data you want to submit after the equals sign (=) sign corresponding to the Name parameter for that data. You may need to view the form in a separate browser window to determine the format and expected values for the Post Data values.

4 Complete the other step settings as necessary. See the section "Settings for URL Sequence Steps" for more information.

5 Click the **Ok** button to add the step.

6 Use the steps in this section to add additional sequence steps. After you have added all the steps to the URL sequence, you must click the **OK** button at the bottom of the properties screen to add the monitor to SiteScope.

Selecting a Frame within a Frameset

Complete the following steps if the URL for a step in the sequence contains an HTML FRAMESET and you need to access a hyperlink, form, or form button that is a page displayed in a frame. You must drill down into the Frameset to the actual page that contains the links or forms that you want before you can proceed with other steps in the sequence.

Selecting an HTML page that is part of a Frameset:

1 Click the radio button to the left of the Frame text entry box.

2 Click the arrow on the right of the box to display all available filenames displayed in the current FRAMESET and then click the file that you want SiteScope to retrieve.

3 Complete the other step settings as necessary. See the section "Settings for URL Sequence Steps" on page 746 for more information.

4 Click the **Ok** button to add the step.

5 Use the steps in this section to add additional sequence steps. After you have added all the steps to the URL sequence, you must click the **OK** button at the bottom of the properties screen to add the monitor to SiteScope.

Following a META REFRESH Redirection

If the page for this step of the sequence is controlled by a <META HTTP-EQUIV="Refresh" CONTENT="timedelay; URL=filename.htm"> tag, you can instruct SiteScope to retrieve the specified file as the next step. This sort of construct is sometimes used for intro pages, splash screens, or pages redirecting visitors from an obsolete URL to the active URL.

To follow a META Refresh redirection:

1. Click the radio button to the left of the Refresh text entry box.
2. Click the arrow on the right of the box to display all available Refresh filenames. Normally there will only be one filename. Select the file that you want SiteScope to retrieve.
3. Complete the other step settings as necessary. See the section "Settings for URL Sequence Steps" on page 746 for more information.
4. Click the **Ok** button to add the step.
5. Use the steps in this section to add additional sequence steps. After you have added all the steps to the URL sequence, you must click the **OK** button at the bottom of the properties screen to add the monitor to SiteScope.

Editing URL Sequence Steps

You can edit the steps in a URL sequence once they have been added. Making changes to a sequence step requires that you update both the individual step and update the monitor as a whole. use the following steps to edit a step in a URL Sequence.

Note: Editing any step of a URL sequence may impact subsequent steps in the sequence and cause the sequence to fail. It may be necessary to change all of the steps that occur after the step that is changed.

To edit a sequence step:

1. In the properties tab for the subject URL Sequence Monitor, click to edit the monitor instance.

2 In the Main Settings section, click the  button to the right of the step you want to edit. The sequence page for that step opens.

3 Edit the settings for the step as necessary.

4 Click the **OK** button at the bottom of the step page to update the step settings. The sequence page closes. The properties view for the monitor is updated with the revised step settings.

5 Click the **OK** button at the bottom of the monitor properties tab to update the monitor. SiteScope will attempt to execute the changes to the step. The results of the monitor run will be displayed in a screen.

Deleting URL Sequence Steps

You can delete steps from a URL sequence but they can only be deleted starting from the last step in the sequence. This is to prevent inadvertently breaking a sequence since, in most cases, one step is dependent on data returned by the previous step. Use the following steps to delete URL sequence steps:

To delete sequence steps:

1 In the properties tab for the subject URL Sequence Monitor, click to edit the monitor instance.

2 In the Main Settings section, click the  button to the right of the step you want to edit. The sequence page for that step opens.

3 Edit the settings for the step as necessary.

4 Click the **OK** button at the bottom of the step page to update the step settings. The sequence page closes. The properties view for the monitor is updated with the revised step settings.

5 Click the **OK** button at the bottom of the monitor properties tab to update the monitor. SiteScope will attempt to execute the changes to the step. The results of the monitor run will be displayed in a screen.

Settings for URL Sequence Steps

The following describes the settings used for each individual sequence step. The scope of each of these settings is limited to the request action for the step. For example, the **User Name** and **Password** settings are only sent as part of the request being made in the step that they are defined.

Reference Type

You use the Reference Type options to select how SiteScope will progress from one step of a URL sequence to the next. The options include:

- **URL** - go to a particular URL directly
- **Link** - follow a hyperlink on the page received from the previous step
- **Form** - enter data into a form received from the previous step and submit the form data to an application
- **Frame** - request the content of a specific frame if the previous step returned an HTML frameset.
- **Refresh** - follow an automated redirection defined by a META HTTP-EQUIV="Refresh" tag.

See the section “Configuring URL Sequence Steps” for more information.

POST Data

If the URL at this step is for a POST request, enter the post variables, one per line as name=value pairs. This option is used to verify that a form is working correctly by performing the same request that occurs when a user submits a form. This item is most commonly used with the *Form* Reference Type. When the form is submitted, SiteScope fills in any items that are not specified with data here with the same defaults as a browser would have chosen.

URL Content Encoding

If the URL content requested in this step uses an encoding that is different than the encoding used on server where SiteScope is running, enter the code page or encoding to use for this step. Some examples of commonly used encodings are: Cp1252, Cp1251, Cp1256, Shift_JIS or EUC_JP. This may be necessary if the default code page which SiteScope is using does not support the character sets used in the target URL. This will enable SiteScope to match and display the encoded content correctly.

Match Content

Enter a string of text to check for in the returned page for this step. If the text is not contained in the page, the monitor will display *no match on content* for this step's URL. The search is case sensitive. Remember that HTML tags are part of a text document, so include the HTML tags and white space if they are part of the text you are searching on. For example, <B> Hello</B> World. You may also perform a regular expression match by enclosing the string in forward slashes, with an *i* after the trailing slash indicating case-insensitive matching (for example, /href=Doc\d+\.html/ or /href=doc\d+\.html/i).

Error If Match

Enter a string of text to check for in the returned page for this step. If the text **is** contained in the page, the monitor will display *no match on content* for this step's URL. The search is case sensitive. Remember that HTML tags are part of a text document, so include the HTML tags if they are part of the text you are searching for (for example, "<B> Error </B> Message"). You may also perform a regular expression match by enclosing the string in forward slashes, with an *i* after the trailing slash indicating case-insensitive matching. (for example, /href=Doc\d+\.html/ or /href=doc\d+\.html/i).

User Name

If the URL specified for this step requires a name and password for access, enter the user name in this box. Alternately, you can leave this entry blank and enter the user name in the Default Authentication Credentials section on the General Preferences page. You use this alternate method to define common authentication credentials for use with multiple Web Service monitor.

Password

If the URL specified for this step requires a name and password for access, enter the password in this box. Alternately, you can leave this entry blank and enter the password in the Default Authentication Credentials section on the General Preferences page. You use this alternate method to define common authentication credentials for use with multiple Web Service monitor.

Authorization NTLM Domain

Enter the domain for NT LAN Manager (NTLM) authorization if it is required in order to access the URL in this step.

Preemptive Authorization

Select when the Authorization User Name and Authorization Password should be sent as part of the URL transaction in this step. The table below describes the options available. By default the setting specified in the Default Authentication Credentials section of the General Preferences page will be used, if they have been specified.

Note: You do not use this setting to control IF the user name and password given for this monitor instance should be sent or WHICH username and password should be sent. You use this setting to select WHEN a username and password should be sent when SiteScope requests the target URL.

Option	Description
Use Global Preference	Select this option to have SiteScope use the **When to Authenticate** setting as specified in the Default Authentication Credentials section of the General Preferences page. **Note:** This only determines when the authorization information is sent. This option will still use the **Authorization User Name** and **Authorization Password** entered for this monitor instance. If these are not specified for the individual monitor, the **Username** and **Password** specified in the Default Authentication Credentials section of the General Preferences page will be used, if they have been specified.
Authenticate first request	Select this option to send the username and password on the first request SiteScope makes for the target URL. This will use the **Authorization User Name** and **Authorization Password** entered for this monitor instance. If these are not specified for the individual monitor, the **Username** and **Password** specified in the Default Authentication Credentials section of the General Preferences page will be used, if they have been specified. **Note:** If the URL does not require a username and password, then this option may cause the URL to fail.
Authenticate if requested	Select this option to send the username and password on the second request if the server requests a username and password. This will use the **Authorization User Name** and **Authorization Password** entered for this monitor instance. If these are not specified for the individual monitor, the **Username** and **Password** specified in the Default Authentication Credentials section of the General Preferences page will be used, if they have been specified. **Note:** If the URL does not require a username and password, then this option may be used.

Step n Delay

(Optional) Enter how long SiteScope should wait before executing the next step of the sequence.

Step n Title

(Optional) Enter the text for the title of this step within the sequence monitor. The title will only be displayed in the Edit URL Sequence form.

URL Sequence Monitor Settings

The following sections describe the settings for the URL Sequence Monitor. These settings apply to all steps that may be defined for the sequence.

Main Settings for the URL Sequence Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the Web transaction, how often this URL Sequence Monitor instance should be run, and the text name used for this monitor instance in the interface. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this URL Sequence monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface. If you do not enter a name text, SiteScope will create a default name based on the host, system, or URL being monitored.

Frequency

Select how often the URL Sequence Monitor should perform the Web transaction. The default interval is to update or run the monitor once every 10 minutes. Use the drop-down list to the right of the text box to specify an update interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Note: Many URL sequences may take a minute or more to complete. Therefore the Frequency should be set to allow enough time for SiteScope to complete the actions of the sequence.

Steps

Use the **Add Step** button to define the URL sequence steps. For details, see "Settings for URL Sequence Steps" on page 746.

URL Content Encoding

While adding URL sequence steps, enter the locale if you are working in an I18N environment. For example, Shift_JIS is the locale string for Japanese. For details, see "URL Content Encoding" on page 747.

Advanced Settings for the URL Sequence Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the URL Sequence Monitor and its display in the product interface. Use this section to set monitor-to-monitor dependencies, customize display options, and configure other settings specific to the URL Sequence Monitor that may be required in some infrastructure environments. Complete the entries as needed.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Timeout

The number of seconds that the URL Sequence Monitor should wait for the entire sequence to complete before timing-out. Once this time period passes, the URL Sequence Monitor will log an error and report an error status.

Timeout is Per Step

Check this box if you want to use the value entered for the Timeout above as the Timeout for each step of the sequence rather than for the entire transaction. If the step takes more than this time to complete, the URL Sequence Monitor will log an error and report an error status.

Retrieve Images

Check this box if you want the status and response time statistics to include the retrieval times for all of the embedded images in the page. Embedded images include those referenced by "IMG" and "INPUT TYPE=IMAGE" HTML tags. Images that appear more than once in a page are only retrieved once.

Note: If the **Retrieve Images** option is checked, each image referenced by the target URL will contribute to the download time. However, if a image times out during the download process or has a problem during the download, that time will not be added to the total download time.

Retrieve Frames

Check this box if you want SiteScope to retrieve the all frames references in a frameset and count their retrieval time in the total time to download this page. If Retrieve Images is also checked, SiteScope will attempt to retrieve all images in all frames.

Note: If the **Retrieve Frames** option is checked, each frame referenced by the target URL will contribute to the download time. However, if a frame times out during the download process or has a problem during the download, that time will not be added to the total download time.

HTTP Proxy

Optionally, a proxy server can be used to access the URLs in the sequence. Enter the domain name and port of an HTTP Proxy Server.

Proxy Server User Name

If the proxy server requires a name and password to access the URLs in the sequence, enter the name here. Technical note: your proxy server must support Proxy-Authenticate for these options to function.

Proxy Server Password

If the proxy server requires a name and password to access the URLs in the sequence, enter the password here. Technical note: your proxy server must support Proxy-Authenticate for these options to function.

Resume at step, if error

You use this option to specify a URL sequence step to execute in the case that a URL Sequence results in an error. This is useful when a URL sequence involves a user or customer login which would result in problems if the sequence were aborted without logging out. Use the drop-down list to select a URL sequence step to jump to in the case that any step in the sequence returns an error.

Execute resume step and remaining steps

If the Resume at step is option is selected and executed, selection of this option causes SiteScope to execute that step and continue executing the other, subsequent steps until it reaches the end of the sequence.

Show Detailed Measurement

Check this box if you want SiteScope to record a detailed break down of the process times involved in retrieving the requested URL. This includes DNS lookup, connect time, HTTP server response time, described as follows:

- **DNS time** - The time it takes to send a name resolution request to your DNS server until you get a reply.
- **Connection time** - The time it takes to establish a TCP/IP/Socket connection to the Web server.
- **Response time** - The time after the request is sent until the first byte (rather first buffer full) of the page comes back.
- **Download time** - The time it takes to download the entire page.

HTTP Version

By default, SiteScope will use HTTP version 1.1 in the request header for URL requests. Some systems may not be designed to accept HTTP 1.1 requests headers. If this is the case, select (check) this option to have SiteScope use HTTP 1.0.

Retries

Enter the number of times, from 0 to 10, to retry the request in the case of recoverable errors. If the monitor times out, the number of retries are cut short.

Accept Untrusted Certs for HTTPS

Select this option to accept certificates that are untrusted in the certificate chain.

Accept Invalid Certs for HTTPS

Select this option to accept certificates even if today's date in not in the date ranges in the certificate chain.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule

➤ Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

➤ Enable all associated alerts

➤ Disable all associated alerts for the next time period

➤ Disable all associated alerts on a one time schedule

➤ Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting URL Sequence Monitor Status Thresholds

SiteScope URL monitor types allow you to set threshold conditions based on part or all of a Web page retrieval or transaction to determine the status reported by each monitor. Monitor status can be set based on the roundtrip, DNS, connect, or response times needed to negotiate a Web request or transaction.

The roundtrip time is one of the most commonly used metrics for URL monitoring. Roundtrip time includes the time to complete the following:

1 Name lookup (DNS)

2 Connect to the server socket

3 Send the HTTP request

4 Download the entire page

If the server hosting SiteScope is heavily loaded, either with other applications or with a significant SiteScope monitoring load, then slower times may be reported, especially for HTTPS URLs, which are more CPU intensive. Usually though, the time waiting for the network is a much greater factor than the CPU usage.

Set the monitor status thresholds for each step of the URL sequence as described below.

Error if

By default, SiteScope generates an error if the returned HTTP status is anything other than 200 ("OK"), which indicates a successful retrieval. You can choose to have SiteScope report an error status based on any of the following measurements:

- round trip time - the total time for the entire request, in milliseconds
- DNS time - the amount of time to translate the host name to an IP address, in milliseconds
- connect time - the amount of time to make the connection, in milliseconds
- response time - the amount of time before the first response was received, in milliseconds
- download time - the amount of time to receive the page contents, in milliseconds
- age -- the amount of time between the current time and the last-modified time for the page, in seconds
- content match
- total errors
- overall status

Choose a comparison operator from the drop-down list, and enter a value for the comparison in the text box.

The URL Monitor follows HTTP redirect codes (301 and 302) to retrieve the actual page before returning the status of the URL retrieval. SiteScope will show a redirect error only if the redirects are more than 10 levels deep - this prevents infinite redirects from being followed, or if the Error On Redirect check box is selected.

Warning if

By default, SiteScope does not generate warnings for URL Sequence Monitors. You may choose to generate a warning based on round trip retrieval time. Enter the shortest retrieval time (in milliseconds) that should generate a warning.

Good if

You can base a good status on the round-trip time for any one step if you want. Select the step from the drop-down list and set the threshold.

When you have successfully defined each step in the sequence that you want to monitor, click the **Ok** button.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the URL Sequence Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see “Common Monitor Settings” in the chapter Chapter 2, “Working with SiteScope Monitors.”

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see “Working with Categories” in *Working with Monitor Administration*.

Retaining and Passing Values Between Sequence Steps

One important feature of the Match Content capability in URL Sequence Monitor is the ability to match, retain and then reference values from one URL sequence step for use as input in a subsequent step. Using one or more sets of parentheses as part of a Match Content regular expression instructs SiteScope to "remember" the values matched by the pattern inside the parentheses. These values can then be referenced using the syntax described in the following example:

Example

Suppose you create a URL Sequence Monitor and include a Match Content expression for the first step to capture some session information. The Step 1 Match Content expression could be in the form of

/[\w\s]*?(*pattern1*)[\/\-\=]*?(*pattern1*)/

The two sets of parentheses in this expression instruct SiteScope to retain the two values matched by *pattern1* and *pattern2*. To use these values as input to the **next** step in the URL sequence, use the syntax {$*valuenum*}. In this example, the string {$1} references the value matched by *pattern1* and {$2} will reference the value matched by *pattern2*.Use the above syntax for passing the referenced values to the URL sequence step immediately following the step in which the content match was made (step 1 to step 2 in our example). You can retain and pass matched values from one step to any other subsequent step by using a compound syntax of {$$*stepnum.valuenum*}. If, in our example, you want to use the value matched by *pattern1*in step 1 as input in a FORM or URL request in step 4 of the URL sequence, you would include the syntax {$$1.1} in Step 4. To reference the value matched by *pattern1*, use the {$$1.2} syntax.

73

Web Server Monitor

The Web Server Monitor reports information about a Web server by reading the server log files. Each time the Web Server Monitor runs, it writes the current hits per minute and bytes per minute in the monitor status string and in the SiteScope logs.

This chapter describes:	On page:
About the Web Server Monitor	761
Configuring the Web Server Monitor	762

About the Web Server Monitor

The information gathered by the Web Server Monitor gives you the ability to see how busy your Web site is. You can use this information to plan hardware upgrades and configuration changes that will improve your visitor's experience.

It is most effective if you create a separate Web Server Monitor for each Web server you are running. If you are running multiple Web servers, each one should have its own log file so that SiteScope can report on them separately. See the section in SiteScope Log File Columns in the SiteScope Reference Guide for information on what data is recorded.

Configuring the Web Server Monitor

The Web Server Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the Web Server Monitor.

Main Settings for the Web Server Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the Web server log, how often this Web Server Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this Web Server monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the Web Server Monitor should server log check the Web server log. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

For SiteScope running on Windows:

The following apply to Web Server Monitors on Windows.

Server

Choose the server where the Web Server you want to monitor is running. Use the drop-down list to select a server from the list of remote servers that are available to the SiteScope agent.

Web Server

Choose the Web server to monitor from the drop-down list. The Web server must be running as a service or daemon to appear in this list. If no server instances are listed, it is also possible the there is an access or account permission mismatch between the SiteScope server and the machine where the Web server is running. If the Web server is not running as a service, you can access the Web server log file directly by entering the path in the **Log File Path** entry in the Advanced section below.

For SiteScope running on UNIX/Linux:

The following apply to Web Server Monitors on UNIX.

Log File Pathname

To monitor Web server statistics on UNIX servers, enter the full pathname of the web server log file. Optionally, you can use a regular expression to insert date and time variables using SiteScope date variables. (for example: s|/firstdir/$shortYear$$0month$$0day$|)

Advanced Settings for the Web Server Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Web Server Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Log File Path

If your Web server does not appear in the Web Server list, you may still monitor it by entering the full path name to the Web server log file. An example of a server log file path is: c:/ns-home/httpd-test/logs/access.

For servers that dynamically generate the filename for log files, you can include regular expression as part of the log file path definition. The SiteScope can then retrieve data from a range of filenames based on evaluation of the regular expressions. For details on regular expressions, see "Using Regular Expressions" in *Advanced Monitor Options*.

Request Size Column

If your Web server saves information in a custom format. Enter the column number which contains the Request Size. If this item is blank, the common log file format is assumed.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set up to ten status thresholds criteria for each status condition per monitor instance. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the Web Server or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.

3 Enter a value applicable to the measurement parameter in the third text box.

4 To add another threshold setting, click the **New Error If** button and repeat the steps above.

5 Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the Web Server Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

74

Web Service Monitor

The Web Service Monitor is used to check Simple Object Access Protocol (SOAP) enabled Web services for availability and stability. The Web Service Monitor sends a SOAP based request to the server and checks the response to verify that the service is responding.

This chapter describes:	On page:
About the Web Service Monitor	769
Configuring the Web Service Monitor	771

About the Web Service Monitor

What to Monitor

You use the Web Service Monitor to check the availability of a Web service accepting Simple Object Access Protocol (SOAP) requests. The Web Service Monitor checks that the service can send a response to the client in certain amount of time and to verify that the SOAP response is correct based on your selected match specifications.

The Simple Object Access Protocol is a way for a program running under one operating system to communicate with another program running under the same or different operating system (such as a Windows 2000 program talking to a Linux based program) The Simple Object Access Protocol uses the Hypertext Transfer Protocol (HTTP) and Extensible Markup Language (XML) for information exchange with services in a distributed environment.

This monitor uses a Web Services Description Language (WSDL) file to extract technical interface details about a Web service and uses information returned to create an actual SOAP request to that Web service. That is this monitor emulates a real Web service client making a request. The SOAP request can be used to confirm that the Web service is serving the expected response data and in a timely manner. The status of the Web Service Monitor is set based on the results of the SOAP request.

You can find more information on SOAP on the W3C Web site at: http://www.w3.org/TR/SOAP/

Information on WSDL is available from Microsoft® at: http://msdn.microsoft.com/xml/general/wsdl.asp

Supported Technologies

The following specification features are currently supported:

- WSDL 1.2
- SOAP 1.1
- Simple and Complex Types based on XML Schema 2001
- SOAP binding with the HTTP(S) protocol only
- SOAP with Attachments is not supported

Note: Be advised that SOAP and WSDL technologies are still undergoing evolution. Consequently there can be instances of WSDL documents that we may not be able to process with complete accuracy. In addition, certain SOAP requests we send may not interact effectively with all Web service providers due to inherent specification ambiguities. However, it is our full intent and commitment to continually keep our implementations up to date with the latest Web service specifications.

Status

The status reading shows the most recent result for the monitor. It is also recorded in the SiteScope log files, e-mail alert messages, and can be transmitted as a pager alert. The possible status values are:

- OK
- unknown host name
- unable to reach server
- unable to connect to server
- timed out reading
- content match error
- document moved
- unauthorized
- forbidden
- not found
- proxy authentication required
- server error
- not implemented
- server busy

The final status result is either OK, error, or warning based on the threshold established for these conditions.

Configuring the Web Service Monitor

The Web Service Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the Web Service Monitor.

Main Settings for the Web Service Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the remote system, how often this Web Service Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this Web Service monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the Web Service Monitor should system check the remote system. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

URL of the WSDL

Enter the URL or the file path of the WSDL file to be used for this monitor. All file paths entered must be relative to the location **<SiteScope install path>/SiteScope/templates.wsdl/**. In addition, your WSDL files must have an extension of *.wsdl*.

File

Optionally you can select a WSDL file from this drop-down list. This list reflects the files found by searching on **<SiteScope install path>/SiteScope/templates.wsdl/*.wsdl**.

Method Name

Select the name of the method to be invoked. During initial setup this will be extracted from the WSDL file.

Pressing on the **Get Methods** button causes the specified WSDL file to be retrieved and analyzed for method arguments. The ensuing screen will display the argument list and structure, if any, that will need actual input values.

Server URL

Shows the URL of the Web service to be monitored. During initial setup this will be extracted from the WSDL file.

Name of arguments

Shows the name and type/structure of the arguments to the method specified above. SiteScope supports both simple (primitive) and complex (user-defined using XML schema) types. Simple type arguments will appear in the form:

parm-name(*parm-type*) =

where you will need to enter the parameter value to be used in invoking the Web service, after the equal sign. Strings with embedded spaces should be enclosed in double quotes. Each parameter must be in a separate line, that is, do not remove the carriage return at the end of each parameter.

A complex type parameter is displayed as one long string, with needed input fields marked with asterisks (***). An example of a complex type parameter is shown below:

```
stocksymbol[COMPLEX] =<stocksymbol
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:fw100="urn:ws-stock"
xsi:type="fw100:getQuote"> <ticker
xsi:type="xsd:string">***</ticker></stocksymbol>
```

You must replace these occurrences of asterisks with meaningful values of the appropriate type (the needed type will be shown, for example, xsd:string above), otherwise the Web service request may fail. Do not add any carriage returns within a complex type parameter.

If the Web service method does not take any parameters, the text box should be empty (and left that way).

Advanced Settings for the Web Service Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Web Service Monitor and its display in the product interface. See “Common Monitor Settings” in the chapter “Working with SiteScope Monitors” for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Match Content

Enter a string of text to check for in the returned page or frameset. If the text is not contained in the page, the monitor will display "no match on content". The search is case sensitive. Remember that HTML tags are part of a text document, so include the HTML tags if they are part of the text you are searching for (for example, "< B> Hello< /B> World"). This works for XML pages as well. You may also perform a regular expression match by enclosing the string in forward slashes, with an "i" after the trailing slash indicating case-insensitive matching. (for example, "/href=Doc\d+\.html/" or "/href=doc\d+\.html/i"). If you want a particular piece of text to be saved and displayed as part of the status, use parentheses in a Perl regular expression. For example /Temperature: (\d+). This would return the temperature as it appears on the page and this could be used when setting an Error if or Warning if threshold

Method Name Space

The XML name space for the method in the SOAP request. During initial setup this value will be extracted from the WSDL file.

Content Type

The SOAP http header content type value. Default is: text/xml; charset="utf-8".

SOAP ACTION

The SOAP ACTION URL in the header of the SOAP request to the Web Service. During initial setup this will be extracted from the WSDL file.

Request's Schema

The request schema. Currently SiteScope only supports SOAP.

HTTP Proxy

Optionally, a proxy server can be used to access the URL. Enter the domain name and port of an HTTP Proxy Server

NTLM Domain Name

If the web service requires NTLM / Challenge Response authentication, a domain name is required as part of your credentials (as well as a user name and password below).

Authorization User Name

If the web service requires a user name and password for access (Basic, Digest or NTLM authentication), enter the user name in this box. Alternately, you can leave this entry blank and enter the user name in the Default Authentication Credentials section on the General Preferences page. You use this alternate method to define common authentication credentials for use with multiple Web Service monitor.

Authorization Password

If the web service requires a user name and password for access (Basic, Digest or NTLM authentication), enter the password in this box. Alternately, you can leave this entry blank and enter the password in the Default Authentication Credentials section on the General Preferences page. You use this alternate method to define common authentication credentials for use with multiple Web Service monitor.

Proxy Server User Name

If the proxy server requires a name and password to access the URL, enter the name here. Technical note: your proxy server must support Proxy-Authenticate for these options to function.

Proxy Server Password

If the proxy server requires a name and password to access the URL, enter the password here. **Technical note** Your proxy server must support Proxy-Authenticate for these options to function.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set one or more status thresholds criteria for each status condition per monitor instance. The status of the monitor and any associated alert action will be set based on comparison of all the threshold criteria you define for the monitor. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the Web Service or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the Web Service Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

75

WebLogic Application Server Monitor

The WebLogic Application Server Monitor allows you to monitor the statistics of a WebLogic version 6 servers and higher. The error and warning thresholds for the monitor can be set on one or more WebLogic server statistics.

This chapter describes:	On page:
About the WebLogic Application Server Monitor	781
Configuring the WebLogic Application Server Monitor	784

About the WebLogic Application Server Monitor

Use the WebLogic Application Server Monitor to monitor performance statistics data from WebLogic 6.x, 7.x, and 8.x servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate WebLogic Application Server Monitor instance for each WebLogic server in your environment.

The BEA WebLogic Application Server monitor uses the Java JMX interface to access Runtime MBeans on the WebLogic server. An MBean is a container that holds the performance data. You must set certain permissions on the WebLogic server for SiteScope to be able to monitor MBeans.

The default run schedule for this monitor is every 10 minutes, but you can change it to run more or less often using the **Frequency** setting.

Configuration Requirements for Monitoring WebLogic 6.x Servers

To set permissions for monitoring WebLogic 6.x servers, create a new ACL on the WebLogic server with the name weblogic.admin.mbean. Set the permission type to access and set the Users and Groups to be the user or group account that SiteScope will use to monitor the WebLogic server.

Configuration Requirements for Monitoring WebLogic 7.x Servers

WebLogic 7.x and later servers use "Security Policies" instead of ACL's to control access to the server resources. In order to be able to monitor WebLogic 7.x servers with SiteScope, the WebLogic administrator will need to add the user account that is running SiteScope to a WebLogic user group. The WebLogic group containing the SiteScope user must then be associated with a "role statement" that will grant the necessary security role for accessing the desired WebLogic resources. The same security role must also be associated with the applicable "policy statement" that will grant SiteScope access to the WebLogic resources. See the WebLogic server documentation for more information.

Configuring SiteScope to Use T3 Over SSL Against a WebLogic Server

You use the following steps to configure a WebLogic Monitor with the **Secure Server** option to monitor a WebLogic 7 or 8 server.

To configure SiteScope to use SSL for WebLogic server monitoring:

1. Obtain and install a JRE version 1.4.1 on the machine where SiteScope is running. Make a note of the full path to this JRE installation as you will need to enter this information in the WebLogic Monitor setup.
2. Import the WebLogic Server's certificate, signed by a certificate authority, into the <*jre_path*>\lib\security\cacerts file for the JRE 1.4.1 installation on the SiteScope machine. If it is not, then you will have to import the signer's certificate into the cacerts file using the keytool program. For instance, using the default WebLogic cert setup, you need to import the CertGenCA.der certificate using the following command (this must all be entered on a single command line):

```
C:\j2sdk1.4.1\jre\bin>keytool.exe -import -alias weblogic81CA -keystore
..\lib\security\cacerts -trustcacerts -file
C:\BEA\weblogic81\server\lib\CertGenCA.der
```

3. Obtain a valid BEA license file and put it somewhere on the SiteScope machine. This is the file named 'license.bea' in the BEA installation directory.
4. Obtain the weblogic.jar file from the WebLogic server or from a WebLogic server of the same version that you will be monitoring. For WebLogic version 8.x, you must also obtain a copy of the wlcipher.jar file. Copy this/these files to the SiteScope server.

Note: Do not install the weblogic.jar file in the SiteScope directory tree. For example, do not install it in the /SiteScope/java/lib/ext directory as this will cause the Weblogic monitor to fail. You must install it in a separate directory on the server where SiteScope is running.

---

5. Open SiteScope and click to add a WebLogic Application Server Monitor.
6. Click the choose server link. Complete the fields in the form as indicated and as described in the following steps.
7. Enter the full path to the javaw.exe (for Windows platforms) or the java (Unix/Linux) executable for the JRE version 1.4.1 installation in the **Location of JVM** field.
8. A valid WebLogic license file must be copied to the SiteScope server. Enter the full path to the BEA license file in the **WebLogic License File** field.
9. Enter the full path to the wlcipher.jar and weblogic.jar files in the **WLCipher Jar File** and the **WebLogic Jar File** fields, respectively.
10. Select the **Secure Server** option.
11. With the other applicable fields completed, you should be able to browse the counters on the WebLogic server over SSL when you click the **Browse Counters** button.

Configuring the WebLogic Application Server Monitor

The WebLogic Application Server Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the WebLogic Application Server Monitor.

Main Settings for the WebLogic Application Server Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the WebLogic server, how often this WebLogic Application Server Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this WebLogic Application Server monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the WebLogic Application Server Monitor should system check the WebLogic server. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Target

Enter the name of the server where WebLogic is running.

Server

Enter the address of the server where WebLogic is running.

Port Number

Enter the port number that the WebLogic server is responding on. The default port is 7001.

User Name

Enter the username required to log into the WebLogic server.

Password

Enter the password required to log into the WebLogic server.

Secure Server

Check this box if you are using a secure server connection option. If you select this option, you must enter the applicable port number used by the WebLogic server for secure connections. The default secure server port is 7002.

WLCipher Jar File

This option is for use only with the **Secure Server** (SSL) option. For some versions of WebLogic Server, you will need to install a copy of the wlcipher.jar file from the WebLogic server onto the SiteScope server to enable monitoring over SSL. You enter the absolute path to the file on the SiteScope machine in this field. For example: C:\bea\weblogic81\server\lib\wlcipher.jar.

Location of JVM

Enter the full path to the Java Virtual Machine (JVM) in which the WebLogic monitoring process should be run. For monitors which will not use the Secure Server option, this is not required. For monitors which do use the Secure Server option, a separate JVM must be installed on the server where SiteScope is running. This other JVM must be version 1.4.1 or earlier. This is not the same JVM version used by SiteScope. An example path might be: C:\j2sdk1.4.1\jre\bin\javaw.exe.

WebLogic License File

You use this field only when you want to enable the Secure Server (SSL) option. Enter the absolute path to the BEA license file that was copied to the SiteScope machine. For example: C:\bea\license.bea.

WebLogic Jar File

Enter the absolute path name to the weblogic.jar file on the SiteScope machine. This file must be installed on the SiteScope server and can be downloaded from the WebLogic server. An example path is: c:\bea\weblogic7\ebcc\lib\ext\weblogic.jar. This file is not strictly required for monitoring some earlier versions of WebLogic 6. In this case, leaving this box blank will normally cause any necessary classes to be downloaded directly from the WebLogic server. Note that this is not as efficient as loading the classes from the *.jar file on the server where SiteScope is running.

Note: Do not install the weblogic.jar file in the SiteScope directory tree. For example, do not install it in the **<SiteScope install path>/SiteScope/java/lib/ext** directory as this will cause the WebLogic monitor to fail. You must create a separate directory on the server where SiteScope is running for this file.

Counters

You use the features associated with the **Counters** setting to choose and manage the metrics you want to monitor with the WebLogic Application Server Monitor. Use the following steps to select and add counters.

To select or add counters:

1. Click **Get Counters** to query the remote system. After SiteScope has successfully connected to the remote system, the Get Counters selection dialogue opens.
2. Use the features in the Get Counters selection dialogue screen to select the WebLogic server metrics you want to monitor. Use the expandable menu controls as applicable to browse the available counters.
3. Use the check boxes to select between one and ten counters to be monitored.
4. Click **OK** to add the selected counters to the monitor configuration. The Get Counters selection dialogue closes and the monitor properties are updated with your selection.

Use the following steps to remove a counter from the selected counters list.

To remove or edit counters:

1. Click to edit the monitor for which you want to remove counters. Alternately, you may select the monitor you want to edit and click the Properties tab and click the **Edit** button. The monitor Properties screen opens.
2. Click the **Get Counters** button to open the Get Counters selection dialogue.
3. Clear the check box to the left of the current counter you want to remove.

   At this point, you may add other counters to the monitor by clicking the applicable check boxes.
4. Click **OK** at the bottom of the screen to update the monitor.

   The performance parameters or counters available for the WebLogic 6.x Application Server Monitor include:

   - MessagesLogged
   - Registered
   - CachingDisabled
   - UnlockedUsersTotalCount
   - InvalidLoginUsersHighCount
   - LoginAttemptsWhileLockedTotalCount
   - Registered
   - LockedUsersCurrentCount
   - CachingDisabled
   - InvalidLoginAttemptsTotalCount
   - UserLockoutTotalCount

   The following categories of measurements also exist for the WebLogic 6.x Application Server Monitor:

   - ServletRuntime
   - WebAppComponentRuntime

- EJBStatefulHomeRuntime
- JTARuntime
- JVMRuntime
- EJBEntityHomeRuntime.
- DomainRuntime
- EJBComponentRuntime
- DomainLogHandlerRuntime
- JDBCConnectionPoolRuntime
- ExecuteQueueRuntime
- ClusterRuntime

Advanced Settings for the WebLogic Application Server Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the WebLogic Application Server Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set one or more status thresholds criteria for each status condition per monitor instance. The status of the monitor and any associated alert action will be set based on comparison of all the threshold criteria you define for the monitor. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the WebLogic Application Server or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the WebLogic Application Server Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

76

WebSphere Application Server Monitor

The WebSphere Application Server Monitor allows you to monitor the availability and server statistics of an IBM WebSphere Application Server 3.5.x, 4.x, and 5.x. The error and warning thresholds for the monitor can be set on one or more WebSphere Application Server performance statistics.

This chapter describes:	On page:
About the WebSphere Application Server Monitor	793
System Requirements	793
Configuring the WebSphere Application Server Monitor	798

About the WebSphere Application Server Monitor

Use the WebSphere Application Server Monitor to monitor the server performance statistics from IBM WebSphere servers using the performance monitoring interfaces provided with WebSphere. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate WebSphere Application Server Monitor instance for each WebSphere Application Server in your environment.

System Requirements

Before you can use the WebSphere Application Server Monitor, there are a number of configuration requirements involving the server environment. The following is an overview of the configuration steps:

For WebSphere 3.5.x and 4.x

Use the following to prepare the WebSphere environment for SiteScope monitoring of WebSphere versions 3.5.x and 4.x.

1 You must first install the IBM WebSphere Administrator's Console on the SiteScope server if you are monitoring WebSphere versions 3.5.x or 4.x. If installing the Administrator's Console:

Select Custom Installation option during installation.

Select **Administrator's Console** and **IBM JDK 1.2.2.** in the **Choose Application Server Components** dialog box.

You will need to specify the machine you want to monitor during the installation.

2 You must enable the WebSphere servers to be monitored. For WebSphere 3.5.x, enable EPM Counters on the WebSphere server. For WebSphere 4.x and 5.x, enable PMI Counters or enable the Performance Monitoring Service on the WebSphere server. You can enable the counters for the application you want to monitor via the WebSphere Administrator's Console.

For WebSphere 4.x, Select Resources and select the Performance option and expand the **Performance Modules** tree in the dialog box that opens. In order to manage different levels of performance data, select the performance modules and choose a performance level. Then click the Set button.

3 Alternatively, on WebSphere 3.5.x, you can set the EPM Specification to:

```
epm=high:epm.beanMethodData=none
```

by using the WebSphere Administrator's Console.

4 If security has been enabled on the WebSphere server, the server security ring must be copied to the admin client.

For WebSphere 5.x

To monitor WebSphere version 5.x the necessary WebSphere libraries must be available on the SiteScope server. Generally, this means that a WebSphere 5.x client install must exist on the SiteScope server.

To install the correct client software on a SiteScope server:

1 Install the following options from the custom options menu in the WebSphere 5.x install:

Administration (or admin console) Performance Analysis

Note: Certain trial versions of IBM WebSphere do not include the Performance Analysis option required by the Sitescope WebSphere Application Server Monitor. The SiteScope monitor will only work when a complete WebSphere production installation is available.

---

2 Copy all of the files from the **lib** folder of a WebSphere 5.x Application Server installation to the **lib** folder on the client install from step 1.

3 The WebSphere 5.x server and client settings have to match. This means that the SiteScope WebSphere Application Server Monitor will not be able to monitor a WebSphere 5.1 application server if the client libraries are from a WebSphere 5.0 and vice versa. Client libraries should be installed in separate folders with clearly distinct directory names (for example, `Websphere50` and `Websphere51`) to avoid confusion and SiteScope setup errors.

4 The `sas.props` file should be replaced with `soap.props` for WebSphere 5.x installations.

Note: For WebSphere 5.x SiteScope uses the WebSphere JMX interface so the port number used to communicate with the application server is the SOAP port number. The default SOAP port number is `8880`.

---

5 You must enable the WebSphere servers to be monitored. For WebSphere 4.x and 5.x, enable PMI Counters or enable the Performance Monitoring Service on the WebSphere server. You can enable the counters for the application you want to monitor via the WebSphere Administrator's Console.

For WebSphere 5.x, Click on **Servers** > **Application Servers**. Select the server to be monitored from the Application Server list. From the Configuration tab, click on the Performance Monitoring Service in the Additional

Properties list. Click the **Start Up** check box and select the **Initial specification** level as Standard or Custom. Then click the Apply button.

6 If security has been enabled on the WebSphere server, the server security ring must be copied to the admin client.

Note: If security has been enabled on the WebSphere server, you must copy the security keyring from the WebSphere server to SiteScope. A keyring is a certification used by the server to identify the client.

For WebSphere 6

To monitor WebSphere version 6 the necessary WebSphere libraries must be available on the SiteScope server. This means that a WebSphere 6 client install must exist on the SiteScope server.

To install the correct client software on a SiteScope server:

1 Install the following options from the custom options menu in the WebSphere 6 install:

Administration (or admin console) Performance Analysis

Note: Certain trial versions of IBM WebSphere do not include the Performance Analysis option required by the Sitescope WebSphere Application Server Monitor. The SiteScope monitor will only work when a complete WebSphere production installation is available.

---

2 Copy all of the files from the **lib** folder of a WebSphere 6 Application Server installation to the **lib** folder of the client installation from step 1.

3 WebSphere 6 server and client settings must match. This means that the SiteScope WebSphere Application Server Monitor will not be able to monitor a WebSphere 6 application server if the client libraries are not from WebSphere 6. Client libraries should be installed in separate folders with distinct directory names (for example, Websphere50, Websphere51, or Websphere6) to avoid confusion and SiteScope setup errors.

4 The **sas.props** file should be replaced with **soap.props** for WebSphere 6 installation.

Note: For WebSphere 5.x and later, SiteScope uses the WebSphere JMX interface so the port number used to communicate with the application server is the SOAP port number. The default SOAP port number is **8880**.

---

5 From the WebSphere Administrator's console, select **Monitoring and Tuning**. This enables PMI counters and enables the Performance Monitoring Service on the WebSphere server.

6 Click **Servers** > **Application Servers** > **Install New Applications**. Choose the **PerfServletApp.ear** file from the installableApps directory.

7 Click **Servers** > **Application Servers**. Select the server to be monitored from the Application Server list.

8 In the Configuration tab, click **Performance Monitoring Service** in the Additional Properties list.

9 Select the **Start Up** check box and select the **Initial specification** level as Standard or Custom.

10 Click **Apply**.

11 If security has been enabled on the WebSphere server, the server security ring must be copied to the admin client.

Note: If security has been enabled on the WebSphere server, you must copy the security keyring from the WebSphere server to SiteScope. A keyring is a certification used by the server to identify the client.

Configuring the WebSphere Application Server Monitor

The WebSphere Application Server Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the WebSphere Application Server Monitor.

Main Settings for the WebSphere Application Server Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the WebSphere server, how often this WebSphere Application Server Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this WebSphere Application Server monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the WebSphere Application Server Monitor should update it's list of selected counters from the WebSphere server. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Server

Choose the server where the WebSphere Application Server you want to monitor is running. Use the drop-down list to select a server from the list of remote servers that are available to the SiteScope agent.

Counters

You use the features associated with the **Counters** setting to choose and manage the metrics you want to monitor with the WebSphere Application Server Monitor. Use the following steps to select and add counters.

To select or add counters:

1. Click **Get Counters** to query the remote system. After SiteScope has successfully connected to the remote system, the Get Counters selection dialogue opens.
2. Use the features in the Get Counters selection dialogue screen to select the WebSphere server metrics you want to monitor. Use the expandable menu controls as applicable to browse the available counters.
3. Use the check boxes to select between one and ten counters to be monitored.
4. Click **OK** to add the selected counters to the monitor configuration. The Get Counters selection dialogue closes and the monitor properties are updated with your selection.

Use the following steps to remove a counter from the selected counters list.

To remove or edit counters:

1. Click to edit the monitor for which you want to remove counters. Alternately, you may select the monitor you want to edit and click the Properties tab and click the **Edit** button. The monitor Properties screen opens.
2. Click the **Get Counters** button to open the Get Counters selection dialogue.
3. Clear the check box to the left of the current counter you want to remove.

   At this point, you may add other counters to the monitor by clicking the applicable check boxes.
4. Click **OK** at the bottom of the screen to update the monitor.

There are a large number of server parameters or counters available for the WebSphere Application Server Monitor. The list of available counters will vary depending on which version of WebSphere you are running. The list of available counters may include:

- MemoryFree
- MemoryTotal
- MemoryUse
- BeanDestroys

- StatelessBeanDestroys
- StatefulBeanDestroys
- NumGetFound
- NumPutsDiscarded
- ActiveThreads
- TotalThreads
- PercentTimeMaxed
- ConnectionWaitTime
- ConnectionTime
- ConnectionPercentUsed
- NumTransactions
- ActiveTransactions
- TransactionRT
- RolledBack
- Timeouts
- TransactionSuspended
- ServletErrors
- SessionsInvalidated

Target

Enter the logical name of the server you want to monitor. If this box is left empty, the hostname entered above will be used.

Advanced Settings for the WebSphere Application Server Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the WebSphere Application Server Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

WebSphere Directory

Enter the path to a WebSphere 3.5x Directory. The directory you enter here should contain at least a valid Admin Client installation.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule

➤ Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

➤ Enable all associated alerts

➤ Disable all associated alerts for the next time period

➤ Disable all associated alerts on a one time schedule

➤ Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set one or more status thresholds criteria for each status condition per monitor instance. The status of the monitor and any associated alert action will be set based on comparison of all the threshold criteria you define for the monitor. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the WebSphere Application Server or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the WebSphere Application Server Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)

- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

77

WebSphere Performance Servlet Monitor

Use the WebSphere Performance Servlet Monitor to monitor the server statistics of IBM WebSphere Server (versions 3.0x, 3.5, 3.5.x, and 4.0) via a WebSphere Performance Servlet. The error and warning thresholds for the monitor can be set on one or more performance statistics.

This chapter describes:	On page:
About the WebSphere Performance Servlet Monitor	807
Configuring the WebSphere Performance Servlet Monitor	808

About the WebSphere Performance Servlet Monitor

The WebSphere Performance Servlet Monitor monitors the server performance statistics for IBM WebSphere servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate WebSphere Performance Servlet Monitor instance for each WebSphere Application Server in your environment.

The following are several key requirements for using the WebSphere Performance Servlet Monitor:

- The WebSphere Performance Servlet is an optional component for WebSphere 3.0x and 3.5x versions. The performance servlet must be installed on WebSphere servers in order to use this monitor. A patch needs to be applied according to which WebSphere 3.x version you are monitoring.
- The WebSphere Performance Servlet must be installed on each WebSphere 3.x server you want to monitor. The files should be copied to

the hosts\default_host\default_app\servlets subdirectory on each WebSphere server machine. The files needed per version are as follows:

- for version 3.02, xml4j.jar, performance.dtd and perf.jar
- for version 3.5, perf35.jar
- for versions 3.5.2 and 3.5.3, perf35x.jar

➤ The WebSphere Performance Servlet should be included as part of WebSphere 4.0 although it needs to be deployed. If you are running WebSphere 4.0 servers, only one instance of the servlet needs to be deployed in order to monitor one or more WebSphere 4.0 servers.

➤ Verify that the servlet is running properly and that the performance data is generated. One way to do this is to try to display it through an XML enabled browser. The servlet URL should be in the following format:

http://<server:port:>/<dir_alias>/com.ibm.ivb.epm.servlet.PerformanceServlet
For example:
http://wbs.company.com:81/servlet/com.ibm.ivb.epm.servlet.PerformanceServlet

Configuring the WebSphere Performance Servlet Monitor

The WebSphere Performance Servlet Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the WebSphere Performance Servlet Monitor.

Main Settings for the WebSphere Performance Servlet Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the WebSphere server, how often this WebSphere Performance Servlet Monitor instance should be run, and the text name used for this monitor instance. See “Common Monitor Settings” in the chapter “Working with SiteScope Monitors” for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this WebSphere Performance Servlet monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the WebSphere Performance Servlet Monitor should system check the WebSphere server. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Target

Enter the logical name of the server that is the target of this monitor instance. If you leave this field empty, the hostname will be used. Depending on the deployment of the WebSphere application in your infrastructure, this may be the same as the **Server** selected below.

Server

Select the server you want to monitor. On UNIX servers, enter the full pathname of the server. You will also be asked to enter the URL to the performance servlet as installed on the WebSphere server and the port number that is to be used to access the server. For WebSphere versions 3.x.x, the URL can be viewed via the Servlet Properties page in the WebSphere Admin Console. For WebSphere version 4.0, the URL normally has the form of http://<server:port_number:>/wasPerfTool/servlet/perfservlet.

Counters

You use the features associated with the **Counters** setting to choose and manage the metrics you want to monitor with the WebSphere Performance Servlet Monitor. Use the following steps to select and add counters.

To select or add counters:

1 Click **Get Counters** to query the remote system. After SiteScope has successfully connected to the remote system, the Get Counters selection dialogue opens.

2 Use the features in the Get Counters selection dialogue screen to select the WebSphere server metrics you want to monitor. Use the expandable menu controls as applicable to browse the available counters.

3 Use the check boxes to select between one and ten counters to be monitored.

4 Click **OK** to add the selected counters to the monitor configuration. The Get Counters selection dialogue closes and the monitor properties are updated with your selection.

Use the following steps to remove a counter from the selected counters list.

To remove or edit counters:

1 Click to edit the monitor for which you want to remove counters. Alternately, you may select the monitor you want to edit and click the Properties tab and click the **Edit** button. The monitor Properties screen opens.

2 Click the **Get Counters** button to open the Get Counters selection dialogue.

3 Clear the check box to the left of the current counter you want to remove.

At this point, you may add other counters to the monitor by clicking the applicable check boxes.

4 Click **OK** at the bottom of the screen to update the monitor.

Advanced Settings for the WebSphere Performance Servlet Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the WebSphere Performance Servlet Monitor and its display in the product interface. See “Common Monitor Settings” in the chapter “Working with SiteScope Monitors” for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Timeout

Enter the time, in seconds, that the monitor should wait for a response from the Performance Servlet. If a response is not received within the interval of the timeout, them monitor will report a timeout error.

Refresh Selected Metrics Frequency

Select a time interval at which the WebSphere server should update the metrics that are requested by this monitor. This value should be equal to or less than the **Frequency** time interval for the monitor.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule

➤ Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

➤ Enable all associated alerts

➤ Disable all associated alerts for the next time period

➤ Disable all associated alerts on a one time schedule

➤ Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set one or more status thresholds criteria for each status condition per monitor instance. The status of the monitor and any associated alert action will be set based on comparison of all the threshold criteria you define for the monitor. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the WebSphere Performance Servlet or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the WebSphere Performance Servlet Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)

- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

78

Windows Services State Monitor

The Windows Services State Monitor is used to monitor a list of services running on Windows NT/2000 systems and report changes in the number of services that are running and list the services that changed state.

This chapter describes:	On page:
About the Windows Services State Monitor	817
Configuring the Windows Services State Monitor	818

About the Windows Services State Monitor

Use the Windows Services State Monitor to monitor the services installed and running on remote Windows servers. By default, the monitor returns a list of all of the services that are set to be run automatically on the remote server. You can filter the list of services returned by the monitor using regular expressions. The monitor displays the number of services running and related statistics along with a summary listing of the services installed on the remote server.

Note: The Windows Services State Monitor only retrieves a list of installed services. It does not query the list of processes that may be running on the remote machine. Use the Service Monitor to monitor processes on remote machines.

Note: At present, the Windows Services State Monitor only signals a change in state for services relative to the previous run of the monitor. This means that if the monitor is set to signal an error if a service has changed from running to not running, the monitor will only signal an error status for one monitor run cycle. The number of services running and not running is reset for each monitor run and this number is used for comparison with the next monitor run. Therefore, in order to effectively use this monitor to generate event alerts, alert definitions associated with this monitor should be configured to alert "Once, after the condition has occurred exactly 1 times."

Configuring the Windows Services State Monitor

The Windows Services State Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the Windows Services State Monitor.

Main Settings for the Windows Services State Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the remote server, how often this Windows Services State Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this Windows Services State monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the Windows Services State Monitor should check running services the remote server. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Server

Choose the server you want to monitor. Use the drop-down list to select a server from the list of remote servers that are available to the SiteScope agent.

Advanced Settings for the Windows Services State Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Windows Services State Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Services to Include

Enter an optional regular expression to filter the list of services returned by the monitor. By default, the monitor will list all of the services detected on the remote machine. When you use a regular expression to filter the list of services, the monitor calculates changes in state (that is, running or not running) based only on the services matched by the regular expression.

Services to Ignore

Enter an optional regular expression to filter the list of services matched by the expression used in the **Services to Include** setting. When you use a **Services to Ignore** regular expression to filter the list of **Services to Include**, the monitor calculates changes in state (that is, running or not running) based only on the services matched by the **Services to Ignore** regular expression.

Include Driver Services

Check this box to have the monitor include all low-level driver services. This will generally increases the size of the list. You use the **Services to Include** and **Service to Ignore** options to filter the list of services returned using this option.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set one or more status thresholds criteria for each status condition per monitor instance. The status of the monitor and any associated alert action will be set based on comparison of all the threshold criteria you define for the monitor. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the Windows Services State or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1 Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.

2 Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.

3 Enter a value applicable to the measurement parameter in the third text box.

4 To add another threshold setting, click the **New Error If** button and repeat the steps above.

5 Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the Windows Services State Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see “Common Monitor Settings” in the chapter Chapter 2, “Working with SiteScope Monitors.”

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see “Working with Categories” in *Working with Monitor Administration*.

79

Windows Dial-up Monitor

The Windows Dial-up Monitor (available only on the Windows NT version of SiteScope) uses the Windows NT Remote Access Service to connect to an Internet Service Provider or Remote Access server and optionally runs a user-defined set of monitors. The monitor confirms that the dial-up connection can be established, and measures the performance of the connection and of the network services using the dial-up connection.

This chapter describes:	On page:
About the Windows Dial-up Monitor	825
Configuring the Windows Dial-up Monitor	827

About the Windows Dial-up Monitor

Because the Windows Dial-up Monitor uses Remote Access, which affects the entire machine's network connectivity when it establishes a connection, it should be used on a machine that is not used for accessing resources outside of the local network. For example, if you were using a Web browser on the machine where SiteScope was running a Windows Dial-up Monitor, and the Windows Dial-up Monitor had connected, all the requests by the browser out to the Internet would also use the dial-up connection, affecting the speed of the browser and the reading from the Windows Dial-up Monitor. The Windows Dial-up Monitor will prevent the other SiteScope monitors (those not being run by this Dial-up Monitor) from running while the dial-up connection is established (they will be held up until the Windows Dial-up Monitor is completed). No two Windows Dial-up Monitors will be run at the same time.

Currently the Windows Dial-up Monitor will use the dial-up connection only for requests outside of the local network. Therefore, if you have monitors that access network resources on the local network, their readings will be the same as if the Windows Dial-up Monitor was not used. However, monitors that access network resources outside the local network will use the dial-up connection. For example, if you ran two Ping monitors in the Windows Dial-up Monitor, one of which was yourserver.com (on the local network), and the other of which was externalserver.com (on an external network), the yourserver.com Ping would be very fast, because it would use the LAN, while the externalserver.com Ping would take longer, because it would go through the dial-up connection.

To set up the Remote Access Service on a Windows NT machine, go to the Network Control Panel, and add the service. At that time you also have the option of adding one or more modems as Remote Access modems. At least one of the modems has to have dial out capability for this monitor to work.

You can use the Windows Dial-up Monitor to measure the performance of your Internet applications from a dial-up user's perspective. The Windows Dial-up Monitor can also be used to monitor the availability and performance of remote access servers.

What to Monitor

If you are primarily interested in dial-up availability, then you can just have the Windows Dial-up Monitor try to connect, and if successful, run one or two low impact monitors to verify that the connection is operating properly. If you are more interested in the perspective of a dialup user, then running a suite of monitors that represent typical user tasks will give you more complete assessment.

About Scheduling this Monitor

Because the Windows Dial-up Monitor stops other monitors from running while it is connected, take into account the number and kinds of monitors that will be running while the connection is established as well as the number of other monitors that are running. If SiteScope is running only Windows Dial-up Monitors, then you can schedule them more frequently (every 5 or 10 minutes). However, if you are monitoring many other items, choose a large interval (hours), so that other monitoring is not disrupted.

Only one Windows Dial-up Monitor can run at a time, so if you have more than one Windows Dial-up Monitor, take that into account when scheduling the monitors.

Status

Each time the Windows Dial-up Monitor runs, it returns a reading and status message and writes them in the monitoring log file.

The reading is the current value returned by this monitor. For example, "5 of 5 monitors OK in 55 sec", or "The line was busy". The status is logged as either OK or warning.

For reports, the Windows Dial-up Monitors saves the total time taken (to connect and run the monitors), the connect time (the time for the modem to establish a physical connection), the authorization time (the time after physical connection is established before the connection can actually be used), and the percentage of the monitors run that were "OK".

Configuring the Windows Dial-up Monitor

The Windows Dial-up Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the Windows Dial-up Monitor.

Main Settings for the Windows Dial-up Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the dial-up system, how often this Windows Dial-up Monitor instance should be run, and the text name used for this monitor instance. See “Common Monitor Settings” in the chapter “Working with SiteScope Monitors” for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this Windows Dial-up monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the Windows Dial-up Monitor should system check the dial-up system. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Phone Number

Type the phone number for the dial-up account, adding any extra modem digits or pauses that are required. For example, 9,4432266 includes a "9," for getting an outside line. Insert a comma wherever you need a short pause.

Account Login

The login name for the dial-up account.

Account Password

The password for the dial-up account.

Monitor(s) to Run

Select the group(s) and/or monitor(s) that you want to run while the dial-up connection is established. Monitors that will be used by Windows Dial-up Monitors should not be scheduled to run by themselves (because then some of their data would be via the dial-up connection, and some of their data would be through the local connection)- make sure that the "Update Every" box for these monitors is blank.

Advanced Settings for the Windows Dial-up Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Windows Dial-up Monitor and its display in the product interface. See “Common Monitor Settings” in the chapter “Working with SiteScope Monitors” for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Timeout

The timeout limits the total time that the Windows Dial-up Monitor takes to connect, authenticate, and run each of it is monitors. If the time ever exceeds this time, then the connection is hung up, and the monitor completes with a timeout error.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set up to ten status thresholds criteria for each status condition per monitor instance. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the Windows Dial-up or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.

3 Enter a value applicable to the measurement parameter in the third text box.

4 To add another threshold setting, click the **New Error If** button and repeat the steps above.

5 Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the Windows Dial-up Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

80

Windows Event Log Monitor

The Windows Event Log Monitor watches one of the Windows Event Logs (System, Application, or Security) for added entries. This monitor is only available on the Windows version of SiteScope.

This chapter describes:	On page:
About the Windows Event Log Monitor	835
Configuring the Windows Event Log Monitor	836

About the Windows Event Log Monitor

The **Run Alerts** setting controls how alerts are triggered by this monitor. If **for each event matched** is chosen, then the monitor triggers alerts for every matching entry found. In this way, the monitor acts much like an event forwarder. If **once, after all events have been checked** is chosen, then the monitor counts up the number of matches and triggers alerts based the **Error If** and **Warning If** thresholds defined for the monitor.

The Windows Event Log Monitor examines only log entries made after the time that the monitor is created. Each time the monitor runs thereafter, it examines only those entries added since the last time it ran. You can choose to filter out messages that are not important by using the fields listed under Advanced Settings to specify values that must appear in the event entry for the entry to match.

When setting up SiteScope alerts for Windows Event Log Monitors that are set to alert "for each event matched", it is most useful to select the NTEventLog template for the e-mail, pager, SNMP, or script alert. This alert template sends the alert with the event entry fields broken out. The type of SiteScope alert triggered depends on the type of the log event entry:

Event Log Entry Type	SiteScope Alert Type
Error	Error
Warning	Warning
Information	OK

Each time the Windows Event Log Monitor runs, it returns a reading and status message and writes them in the **<SiteScope install path>/SiteScope/logs/SiteScope*yyyy_mm_dd*.log** file.

Status

The status for the Windows Event Log Monitor includes the number of entries examined, and the number of entries matched. If an interval is specified, the number of events in that interval is also displayed. Matched entries and interval entries can trigger alerts.

Configuring the Windows Event Log Monitor

The Windows Event Log Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the Windows Event Log Monitor.

Main Settings for the Windows Event Log Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the Windows event log, how often this Windows Event Log Monitor instance should be run, and the text name used for this monitor instance. See “Common Monitor Settings” in the chapter “Working with SiteScope Monitors” for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this Windows Event Log monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the Windows Event Log Monitor should event log check the Windows event log. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Server

Choose the server that you want to monitor. The default is to monitor an event log on this server. To monitor the event log on another server, use the drop-down list to select a server from the list of remote servers that are available to the SiteScope agent.

Log Name

Choose either the Application, System, or Security Event Log.

Event Type

Select the event type(s) - Error, Warning, and/or Information - that you are looking for.

Run Alert

Select the method for running alerts. If **for each event matched** is chosen, then the monitor triggers alerts for every matching entry found. If **once, for all events** is chosen, then the monitor counts up the number of matches and triggers alerts based the **Error If** and **Warning If** thresholds defined for the monitor.

Advanced Settings for the Windows Event Log Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Windows Event Log Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Source and ID Match

Enter the match string identifying the source of the event and the event ID in the form: Event Source:Event ID. For example, enter Print:20 to match event source named Print and event ID of 20. To match against all events from a specific source, enter just the event source name (for example: W3SVC). To match an exact event ID from an event source, specify both (for example: Service Control Mar:7000). You can also use a regular expression for more complex matches.

Source and ID NOT Match

Enter the match string identifying the source of the event NOT TO MATCH in the form: Event Source:Event ID. For example, enter Print:20 will ignore all events of Print source and event ID 20. To ignore all events from for a particular source specify just the source name: W3SVC). To ignore an exact event ID from an event source, specify both (for example: Service Control Mar:7000). You can also use a regular expression for more complex not matches. For example, to ignore all Perflib sources from 200 to 299 the following would be used: /Perflib:2\d\d/. To ignore all events from the Perflib source the following would be used: Perflib:*.

Description Match

Enter the text string to match against the description text for the event entry. The description text is the same as the description that is displayed when viewing the detail of an event log entry in the Windows Event Viewer. You can also enter a regular expression in this field to match on patterns.

Description Not Match

Negative match against the description text for the event entry - that is, the Windows Event Log Monitor will trigger an alert only if the text entered in this box **does not** appear in the event entry's description text. The description text can be viewed in the detail view of the event log entry via the Windows Event Viewer. You can also enter a regular expression in this field to match on patterns.

Event Category

Match the category number of the event entry.

Event Machine

Match against the machine that added the entry to the log file.

Interval

Enter an time period, in minutes, for which matching event log entries will be totaled. This is useful when the case you are interested in is a quantity of events happening in a given time period. For example, if you wanted to detect a succession of service failures, 3 in the last 5 minutes, you would specify 5 minutes for the interval, and then change the **Error If** threshold to *matches in interval >= 3*.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set up to ten status thresholds criteria for each status condition per monitor instance. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the Windows Event Log or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the Windows Event Log Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

81

Windows Performance Counter Monitor

The Windows Performance Counter Monitor tracks the values of any Windows performance statistic. These are the same statistics that can be viewed using the "Performance Monitor" application under Windows . This monitor is only available on the Windows version of SiteScope.

This chapter describes:	On page:
About the Windows Performance Counter Monitor	845
Configuring the Windows Performance Counter Monitor	845

About the Windows Performance Counter Monitor

Each time the Windows Performance Counter Monitor runs, it returns a reading and a status message and writes them in the monitoring log file. The status is displayed in the group detail table for the monitor which represents the current value returned by this monitor. For example, 1.24 Interrupts/sec. The status is logged as either OK or warning. An error occurs if the counter could not be read.

Configuring the Windows Performance Counter Monitor

The Windows Performance Counter Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the Windows Performance Counter Monitor.

One way to fill in the boxes for an Windows Performance Counter Monitor is to open up the "Performance Monitor application, click "Add To Chart...", and browser to find the performance measurement that you want the monitor to make. Setting files (ending in .pmc or pmw) from the Windows Performance Counter Monitor can be used to specify which counters you want to monitor.

Main Settings for the Windows Performance Counter Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the system, how often this Windows Performance Counter Monitor instance should be run, and the text name used for this monitor instance. See “Common Monitor Settings” in the chapter “Working with SiteScope Monitors” for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this Windows Performance Counter monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the Windows Performance Counter Monitor should system check the system. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Server

Choose the server that you want to monitor. The default is to monitor a performance counter on this server. TO monitor counters on another server, use the drop-down list to select a server from the list of remote servers that are available to the SiteScope agent. When using a setting file from the Windows Performance Counter Monitor, all counters will be measured on the server specified by this entry.

Perfmon Chart File

Select the Windows Performance Counter Monitor setting file you want to use for your settings. These files can be saved in the Windows Performance Counter Monitor (perfmon) and have either a .pmc or .pmw extension. On Windows 2000 Platform these can be saved using the .htm format. The files in this list all reside in the **<SiteScope install path>/SiteScope/templates.perfmon** directory under SiteScope. There are a number of default files in the standard SiteScope distribution.

Note: If you make your own settings file, it will need to be placed in the **<SiteScope install path>/SiteScope/templates.perfmon** directory. You can optionally specify the settings directly for a single counter below under the Advanced Settings section.

If you create your own .pmc file, it is important to note that any server specified in the .pmc file will be ignored by SiteScope. The server to be queried will be the one selected via the **Server** selection box on monitor setup page (see above). Therefore, you should not include identical counters directed at different servers in a single .pmc file. One .pmc file can be used by more than one Windows Performance Counter Monitor instance but any single instance of the Windows Performance Counter Monitor will only query one server regardless of the servers assigned in the .pmc.

If you have specified the settings directly in the Advanced Settings section, this list will display "(Custom Object)".

Advanced Settings for the Windows Performance Counter Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Windows Performance Counter Monitor and its display in the product interface. See “Common Monitor Settings” in the chapter “Working with SiteScope Monitors” for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Object

The Object is the same as the "Object" in the Performance Monitor application - just type it in this box. The Object is the high level item that will be measured, such as Processor or Server. Note that the object name is case-sensitive. If you are using a Performance Monitor file for counter settings, leave this item blank.

Counter

The counter is the same as the "Counter" in the Performance Monitor application - just type it in this box. The Counter is the specific aspect of the Object that will measured, such as Interrupts/sec. Note that the counter name is case-sensitive. If you are using a Performance Monitor file for counter settings, leave this item blank.

Instance

Some counters can have multiple instances - for example, on machines with two CPUs, there are two instances of the Processor object. The instance is the same as the "Instance" in the Performance Monitor application - just type it in this box. Note that the instance name is case-sensitive. If you are using a Performance Monitor file for counter settings, leave this item blank.

Units

If you want units to be displayed with the counter's values to make them more readable, enter the units here.

Scale

If you want the raw performance counter value scaled to make it more readable, select the scale here. The raw value of the counter will be multiplied by the scale to determine the value of the monitor. The kilobytes option divides the raw value by 1,024 (the number of bytes in 1 K), and the megabytes option divides the raw value by 1,048,576 (the number of bytes in 1 MB). If there are multiple counters specified via a Performance Monitor file, this scaling applies to all counters.

Baseline Interval

Enter the number of monitor runs to be averaged for use as a Rolling Baseline. Rolling baselines are calculated for an interval equal to time to complete the number of monitor runs entered here. For more information, see Setting up and Using Rolling Baselines.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set up to ten status thresholds criteria for each status condition per monitor instance. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the Windows Performance Counter or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.

3 Enter a value applicable to the measurement parameter in the third text box.

4 To add another threshold setting, click the **New Error If** button and repeat the steps above.

5 Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the Windows Performance Counter Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

82

Windows Media Player Monitor

The Windows Media Player Monitor allows you to emulate a user playing media or streaming data from a Windows Media Server. The error and warning thresholds for the monitor can be set on one or more Windows Media Player performance statistics.

This chapter describes:	On page:
About the Windows Media Player Monitor	855
Configuring the Windows Media Player Monitor	856

About the Windows Media Player Monitor

Use the Windows Media Player Monitor to monitor availability and delivery quality parameters for media files and streaming data compatible with Windows Media Servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to report on delivery performance. Create a separate monitor instance for files or data streams that are representative of the content available from the site you want to monitor.

Note: You should only monitor video, not audio, streams with this monitor.

You must have an instance of Windows Media Player installed on the machine where SiteScope is running in order to use this monitor.

The default run schedule for this monitor is every 10 minutes, but you can change it to run more or less often using the **Frequency** setting.

Configuring the Windows Media Player Monitor

The Windows Media Player Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the Windows Media Player Monitor.

Main Settings for the Windows Media Player Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the Windows Media Player, how often this Windows Media Player Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this Windows Media Player monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the Windows Media Player Monitor should check the Windows Media Player. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

URL

Enter the URL of the media file or streaming source you want to monitor. This should be the URL of the media file. For example: mms://*servername*/sample.asf for a unicast stream or http://*servername*/*stationid*.nsc for a multicast stream using a Windows Media Server multicast station program. This monitor does not support the .asx or .mov formats.

Counters

Select the media player performance parameters or counters you want to check with this monitor. The table list to the right of this item displays those currently selected for this monitor. Click **Get Counters** to bring up the counters selection screen. Check or clear the check boxes on the Get Counters screen to select one or more counters to monitor on this server. The performance parameters or counters available for the Windows Media Player Monitor include:

- packet quality - The percentage ratio of packets received to total packets
- time quality - The percentage of stream samples received on time (no delays in reception)
- stream count - The packet count.
- stream rate - The packet rate, indicating the speed at which the clip is played. "1" is the actual speed, "2" is twice the original speed, etc.
- buffering count - The number of times the Player had to buffer incoming media data due to insufficient media content
- buffering time - The time spent waiting for sufficient media data in order to continue playing the media clip
- interrupts - The number of interruptions encountered while playing a media clip. Includes buffering and playback errors.
- packets lost - The number of lost packets not recovered (applicable to network playback).
- packets recovered - The number of lost packets successfully recovered (applicable to network playback).
- ratio bandwidth - The ratio of the actual bandwidth to the recommended bandwidth.
- recommended bandwidth - The recommended bandwidth in bits per second.
- recommended duration - The total duration of the media clip in seconds. This value is not effected by what was already played.
- sampling rate - The sampling rate in milliseconds, for collecting statistics.
- stream max - The maximum number of packets.

➤ stream min - The minimum number of packets

Duration

Enter the playback duration (in milliseconds) that the monitor should use for the media file or source indicated by the **URL** above. The duration value does not need to match the duration of the media contained in the file. For example, you can direct SiteScope to monitor a media file that contains 45 seconds of media content. The default **Duration** for the Real Media Player Monitor is 15000 milliseconds which equals 15 seconds. In this configuration, the monitor instance would connect to the media source and play the media content for 15 seconds and report the status for those 15 seconds. If the media content of the file or source you are monitoring is less than the **Duration** value selected for the monitor, the monitor plays the entire media content and reports the results, including the time required to play the media content.

Advanced Settings for the Windows Media Player Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Windows Media Player Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set one or more status thresholds criteria for each status condition per monitor instance. The status of the monitor and any associated alert action will be set based on comparison of all the threshold criteria you define for the monitor. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the Windows Media Player or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the Windows Media Player Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

83

Windows Media Server Monitor

The Windows Media Server Monitor allows you to monitor the availability of a Microsoft Windows Media server on Windows NT systems. The error and warning thresholds for the monitor can be set on one or more Windows Media server performance statistics.

This chapter describes:	On page:
About the Windows Media Server Monitor	863
Configuring the Windows Media Server Monitor	864

About the Windows Media Server Monitor

Use the Windows Media Server Monitor to monitor the server performance parameters for Microsoft Windows Media Servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate monitor instance for each Windows Media Server you are running.

The Windows Media Server Monitor makes use of Performance Counters to measure application server performance. SiteScope will need to be running under an account that has the necessary administrative security privileges to access performance counter data from remote servers. If the servers you want to monitor are in a different domain, are governed under a different policy, or require a unique login different than the account SiteScope is running under, then you will need to define the connection to these servers under the Windows Servers container in the SiteScope Preferences.

The default run schedule for this monitor is every 10 minutes, but you can change it to run more or less often using the **Frequency** setting.

Configuring the Windows Media Server Monitor

The Windows Media Server Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the Windows Media Server Monitor.

Main Settings for the Windows Media Server Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the Windows media server, how often this Windows Media Server Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this Windows Media Server monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the Windows Media Server Monitor should server check the Windows media server. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Server

Choose the server where the Windows Media Server you want to monitor is running. Use the drop-down list to select a server from the list of remote servers that are available to the SiteScope agent.

Counters

You use the features associated with the **Counters** setting to choose and manage the metrics you want to monitor with the Windows Media Server Monitor. Use the following steps to select and add counters.

To select or add counters:

1. Click **Get Counters** to query the remote system. After SiteScope has successfully connected to the remote system, the Get Counters selection dialogue opens.
2. Use the features in the Get Counters selection dialogue screen to select the Windows media server metrics you want to monitor. Use the expandable menu controls as applicable to browse the available counters.
3. Use the check boxes to select between one and ten counters to be monitored.
4. Click **OK** to add the selected counters to the monitor configuration. The Get Counters selection dialogue closes and the monitor properties are updated with your selection.

Use the following steps to remove a counter from the selected counters list.

To remove or edit counters:

1. Click to edit the monitor for which you want to remove counters. Alternately, you may select the monitor you want to edit and click the Properties tab and click the **Edit** button. The monitor Properties screen opens.
2. Click the **Get Counters** button to open the Get Counters selection dialogue.
3. Clear the check box to the left of the current counter you want to remove.

   At this point, you may add other counters to the monitor by clicking the applicable check boxes.
4. Click **OK** at the bottom of the screen to update the monitor.

The performance parameters or counters available for the Windows Media Server Monitor include:

- Active Live Unicast Streams
- Active Streams

- Active TCP Streams
- Active UDP Streams
- Aggregate Read Rate
- Aggregate Send Rate
- Connected Clients
- Connection Rate
- Controllers
- HTTP Streams
- Late Reads
- Pending Connections
- Stations
- Streams
- Stream Errors

Advanced Settings for the Windows Media Server Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Windows Media Server Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set one or more status thresholds criteria for each status condition per monitor instance. The status of the monitor and any associated alert action will be set based on comparison of all the threshold criteria you define for the monitor. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the Windows Media Server or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the Windows Media Server Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

84

Windows Resources Monitor

The Windows Resources Monitor allows you to monitor system performance data using the Performance Data Helper (PDH) interface on Windows NT/2000 systems. The error and warning thresholds for the monitor can be set on one or more performance statistics.

This chapter describes:	On page:
About the Windows Resources Monitor	871
Configuring the Windows Resources Monitor	872

About the Windows Resources Monitor

Use the Windows Resources Monitor to monitor the server performance statistics from remote NT/2000 servers. This allows you to watch server loading for performance, availability, and capacity planning. You can monitor multiple parameters or counters on a single, remote server with each monitor instance. Create one or more Windows Resources Monitor instances for each remote server in your environment.

The Windows Resources Monitor makes use of Performance Counters to measure application server performance. SiteScope will need to be running under an account that has the necessary administrative security privileges to access performance counter data from remote servers. If the servers you want to monitor are in a different domain, are governed under a different policy, or require a unique login different than the account SiteScope is running under, then you will need to define the connection to these servers under the Windows Remote Preferences option in the SiteScope Preferences container.

The default run schedule for this monitor is every 10 minutes, but you can change it to run more or less often using the **Frequency** setting.

Configuring the Windows Resources Monitor

The Windows Resources Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the Windows Resources Monitor.

Main Settings for the Windows Resources Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the system, how often this Windows Resources Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this Windows Resources monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the Windows Resources Monitor should system check the system. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Server

Choose the server you want to monitor. Use the drop-down list to select a server from the list of remote servers that are available to the SiteScope agent.

Measurements

You use the features associated with the Measurements option to choose and manage the server system measurements you want to check with the Windows Resources Monitor. A list to the right of this item displays the measurements currently selected for this monitor. Use the following steps to select and add measurements:

To select or add measurements:

1. Click the **Get Measurements** button to open the measurements selection panel.
2. Use the **Objects** drop down menu to select the system object for which you want to take measurements. The measurements selection panel is updated with the data relevant to the selected object.
3. If there is more than one instance of the type of object you have selected, use the check boxes in the **Instances** section to select the instance for which you want to take measurements.
4. Use the check boxes on the **Counters** section to select one or more measurements to monitor for the selected object and instance.
5. Click the **Add** button to add the selected measurements to the monitor configuration.
6. Repeat the steps above to add measurement counters for other objects on the remote server.

Use the following steps to remove a measurement counter from the selected measurements list.

To remove measurements:

1. Click to edit the monitor for which you want to remove measurement counters. Alternately, you may select the monitor you want to edit and click the Properties tab and click the **Edit** button. The monitor Properties screen opens.
2. Use the check boxes to the left of the current counters in the Measurements section to select which measurements you want to remove. The list is updated.

At this point, you may add new measurements to the monitor by clicking the **Get Measurements** button and selecting the new measurement objects and counters.

3 Click the **X** button below the list to remove the measurements from the list. Click the **Ok** button at the bottom of the screen to update the monitor.

The performance parameters or counters available for the Windows Resources Monitor will vary depending on what operating system options and applications are running on the remote server. Some examples of Objects available to the Windows Resources Monitor include:

Object Names

- ACS/RSVP Service
- Active Server Pages
- Browser Cache
- Distributed Transaction Coordinator
- FTP Service
- Http Indexing Service
- IAS Accounting Clients
- IAS Accounting Server
- IAS Authentication Clients
- IAS Authentication Server
- ICMP
- IP
- Indexing Service
- Indexing Service Filter
- Internet Information Services Global
- Job Object
- Job Object Details
- Objects
- Paging File
- PhysicalDisk
- Print Queue
- Process
- Processor
- RAS Port
- RAS Total
- Redirector
- SMTP NTFS Store Driver
- SMTP Server
- Server
- Server Work Queues
- System
- TCP
- Telephony
- Terminal Services

- LogicalDisk
- Memory
- NBT Connection
- Network Interface
- Terminal Services Session
- Thread
- UDP
- Web Service

Advanced Settings for the Windows Resources Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Windows Resources Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set one or more status thresholds criteria for each status condition per monitor instance. The status of the monitor and any associated alert action will be set based on comparison of all the threshold criteria you define for the monitor. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the Windows Resources or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the Windows Resources Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

85

XML Metrics Monitor

The XML Metrics Monitor allows you to monitor metrics for systems that make performance data available in the form of an XML file or page. The error and warning thresholds for the monitor can be set on one or more different objects.

This chapter describes:	On page:
Working with the XML Metrics Monitor	881
Configuring the XML Metrics Monitor	882

Working with the XML Metrics Monitor

The XML Metrics Monitor operates like many other browsable monitors: it gathers information from a source, organizes it into a browsable tree structure, and allows the user to choose which items in the tree should be monitored. It works by requesting an XML file that is accessible by an URL.

When defining the monitor, the XML metrics file will be parsed for a list of counters. SiteScope will display a browse tree of counters for you to choose the metrics you want to monitor. When the monitor runs, the XML metrics file is parsed to extract values for each of the counters selected during setup.

System Requirements

A monitor instance must be defined and run against the same XML metrics file format. That is, when running this monitor SiteScope expects the XML file it is monitoring to have the same format that was used when defining that monitor.

SiteScope parses the input XML content according to the following assumptions:

- The XML content has only one root node. This means that all of the XML content is encapsulated within a single parent element and not multiple instances of a repeating root element.
- A leaf node (that is, an element containing only character data and no child elements) is considered a "counter" and must be of the form:

  <node_tag>node_value</node_tag>

  where <node_tag> becomes the counter name, and node_value is reported as the counter value.
- Each leaf node (and therefore each counter) must have a unique path within the hierarchy of the XML content.
- The XML metric file should contain at least one leaf node.

If your XML metric file does not conform to these rules, you can specify a XSLT file (stands for: eXtensible Stylesheet Language: Transformations) that transforms your XML into one that does. Such a file usually has a file extension of .xsl.

If you need to develop a XSLT file to transform the XML content for this monitor, SiteScope includes a Tools page you can use to verify the transformation output. See the "XML Transform Test" in the section "Tools for Troubleshooting" for more information.

The default run schedule for this monitor is every 10 minutes, but you can change it to run more or less often using the Frequency setting.

Configuring the XML Metrics Monitor

The XML Metrics Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the XML Metrics Monitor.

Main Settings for the XML Metrics Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the XML URL, how often this XML Metrics Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this XML Metrics monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the XML Metrics Monitor should check the XML URL. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Authorization User Name

If the URL with the XML content you want to monitor requires a user name and password to access it, enter the user name in this box.

Authorization Password

If the URL with the XML content you want to monitor requires a name and password for access, enter the password in this box.

Proxy Server

Optionally, if you must use a proxy server to access the XML URL, enter the host or domain name and port of the proxy server in this box.

Proxy Username

If you use a proxy server and the proxy requires a name and password to access the target URL, enter the user name in this box.

Note: The proxy server must support Proxy-Authenticate for these options to function.

Proxy Password

If the proxy server requires a name and password to access the URL, enter the password here.

Note: The proxy server must support Proxy-Authenticate for these options to function.

XML URL

Enter the URL of the XML page or file that contains the metrics that you want to monitor.

XSL File

Optional transform file that will be used to convert the above XML metrics file into a format that SiteScope can use. See the section "Working with the XML Metrics Monitor" on page 881 for format rules.

Counters

Choose the counters (objects) you want to check with this monitor. The table list to the right of this item displays those currently selected for this monitor. Click **Get Counters** to bring up the counters selection screen. Check or clear the check boxes on the Get Counters screen to select one or more counters to monitor on this server.

Advanced Settings for the XML Metrics Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the XML Metrics Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Timeout

The number of seconds that the monitor should wait the XML page to complete downloading before timing-out. Once this time period passes, the monitor will log an error and report an error status.

Authorization NTLM Domain

Enter the domain for NT LAN Manager (NTLM) authorization if it is required in order to access the URL.

Preemptive Authorization

Select when the Authorization User Name and Authorization Password should be sent as part of the URL transaction. The table below describes the options available. By default the setting specified in the Default Authentication Credentials section of the General Preferences page will be used, if they have been specified.

Note: You do not use this setting to control IF the user name and password given for this monitor instance should be sent or WHICH username and password should be sent. You use this setting to select WHEN a username and password should be sent when SiteScope requests the target URL.

Option	Description
Use Global Preference	Select this option to have SiteScope use the **When to Authenticate** setting as specified in the Default Authentication Credentials section of the General Preferences page. **Note:** This only determines when the authorization information is sent. This option will still use the **Authorization User Name** and **Authorization Password** entered for this monitor instance. If these are not specified for the individual monitor, the **Username** and **Password** specified in the Default Authentication Credentials section of the General Preferences page will be used, if they have been specified.

Option	Description
Authenticate first request	Select this option to send the username and password on the first request SiteScope makes for the target URL. This will use the **Authorization User Name** and **Authorization Password** entered for this monitor instance. If these are not specified for the individual monitor, the **Username** and **Password** specified in the Default Authentication Credentials section of the General Preferences page will be used, if they have been specified. **Note:** If the URL does not require a username and password, then this option may cause the URL to fail.
Authenticate if requested	Select this option to send the username and password on the second request if the server requests a username and password. This will use the **Authorization User Name** and **Authorization Password** entered for this monitor instance. If these are not specified for the individual monitor, the **Username** and **Password** specified in the Default Authentication Credentials section of the General Preferences page will be used, if they have been specified. **Note:** If the URL does not require a username and password, then this option may be used.

Accept Untrusted Certs for HTTPS

Check this option if you need to use certificates that are untrusted in the cert chain in order to access the target XML URL using Secure HTTP (HTTPS).

Accept Invalid Certs for HTTPS

Check this option if you need to accept an invalid certificate in order to access the target XML URL using Secure HTTP (HTTPS). This may happen, for example, if the current date is not in the date ranges specified in the certificate chain.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set one or more status thresholds criteria for each status condition per monitor instance. The status of the monitor and any associated alert action will be set based on comparison of all the threshold criteria you define for the monitor. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the XML Metrics or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the XML Metrics Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

Part IV

Optional Monitors

86

Active Directory Replication Monitor

The SiteScope Active Directory Replication Monitor allows you to monitor the time that it takes replication to occur between up to ten Domain Controllers. The error and warning thresholds for the monitor can be set on each of the monitored Domain Controllers.

This chapter describes:	On page:
About the Active Directory Replication Monitor	895
Editing the Active Directory Replication Monitor	896

Note: The Active Directory Replication Monitor is an optional SiteScope feature. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your Mercury sales representative for more information.

About the Active Directory Replication Monitor

Use the Active Directory Replication Monitor to monitor the time that it takes a change made on one Domain Controller to replicate to up to as many as ten other Domain Controller. This allows you to verify that replication, a key part of the Active Directory System, is occurring within set thresholds. Create a separate Active Directory Replication Monitor for each Domain Controller that is being replicated throughout your system.

No additional setup is required other than to allow access to a Domain Admin account.

The Active Directory Replication Monitor works by making a small change to part of the Directory Service tree of the configured Domain Controller. It then checks each of the configured Replicating Domain Controllers for this small change. As the change is detected the difference between when the change was made and when it was replicated is computed.

The default run schedule for this monitor is every 10 minutes, but you can change it to run more or less often using the **Frequency** setting.

Editing the Active Directory Replication Monitor

The Active Directory Replication Monitor is part of the Active Directory Solution. This monitor type can only be added by deploying an Active Directory Solution template. Once the monitor has been created, you can edit the configuration of the monitor the same as other monitors. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the Active Directory Replication Monitor.

Main Settings for the Active Directory Replication Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the domain controller, how often this Active Directory Replication Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this Active Directory Replication monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the Active Directory Replication Monitor should system check the domain controller. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Domain Controller

Select the Domain Controller that will contain the replicated data.

Replicating Domain Controllers

Enter a comma separated list of Domain Controllers that replicate data from the Domain Controller entered above.

Username

Enter either the Username or entire Security Principal of a Domain Admin account. If a Username is given the default security principal is created from the root context of the Domain Controller. For Example: If you enter in Administrator for a domain controller in the yourcompany.com domain then the entire Security Principal would be CN=Administrator,CN=Users,DC=yourcompany,DC=com.

Password

Enter the password for the Domain Admin account.

Maximum Replication Time

Enter the maximum amount of time for replication to occur. The monitor will go into error if any of the Replicating Domain Controllers exceed this replication time.

Advanced Settings for the Active Directory Replication Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Active Directory Replication Monitor and its display in the product interface. See “Common Monitor Settings” in the chapter “Working with SiteScope Monitors” for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Polling Interval

The amount of time this monitor should wait between queries of the Replicating Domain Controllers. A higher number reduced the number of LDAP queries against the servers.

Path to Directory

The path to a Directory in the Active Directory that you want to monitor. This is in the form of a LDAP query. The default is based off the default Directory for this server. For example: The default for a Domain Controller for sub.yourcompany.com would be DC=sub,DC=yourcompany,DC=com.

Trace

This will turn on detailed tracing of the LDAP queries being executed. Only needed to debug problems.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set one or more status thresholds criteria for each status condition per monitor instance. The status of the monitor and any associated alert action will be set based on comparison of all the threshold criteria you define for the monitor. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the Active Directory Replication or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the Active Directory Replication Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

87

COM+ Server Monitor

You use the COM+ Server Monitor to monitor the performance of software components registered and running on Microsoft COM+ servers. When you specify the host and port number of this probe instance, SiteScope will retrieve all the functions running on the COM+ server, for your monitoring selection. Error and warning thresholds for the monitor can be set on one or more function measurements.

This chapter describes:	On page:
About the COM+ Server Monitor	903
COM+ Probe Installation	904
Configuring the COM+ Server Monitor	905

Note: The COM+ Server Monitor is an optional SiteScope feature. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your Mercury sales representative for more information.

About the COM+ Server Monitor

The following are several key requirements for using the COM+ Server Monitor:

- A COM+ probe component from Mercury Interactive must be installed and running on the target COM+ server you want to monitor.

- There must be HTTP connectivity between the SiteScope server and the server running the COM+ probe.
- To enable this monitor type in SiteScope, an Option license for the COM+ Monitor must be obtained and input into SiteScope.

Note: You cannot have multiple SiteScope instances share one probe instance. You can have multiple COM+ monitors within a single SiteScope installation access the same probe instance (uniquely identified by the probe host and port). The probe cannot serve data to multiple SiteScope installations.

COM+ Probe Installation

The COM+ probe is available from the Mercury Interactive Customer Support download site. You will need a login to this Mercury Interactive CSO site to access the Customer Support Downloads page. If you do not have one, go to the Mercury Interactive Support site and register. After logging in, click the "Customer support downloads" radio button found in the "Show Me Articles..." box on the lower left corner of the page. Select product "SiteScope", then click the "RETRIEVE" button. You should see a list of downloads and a link that identifies the COM Plus Server Monitor Add In component.

After downloading, follow the instructions for installing the probe on the COM+ server to be monitored.

Once the probe is successfully installed you must start it prior to running or defining a SiteScope COM+ monitor, by invoking the file mon_cplus_probe.exe found in the COM+ probe's bin directory. By default the installation creates this file at:

C:\Program Files\Mercury Interactive\COMPlus Monitor\bin\mon_cplus_probe.exe

COM+ Functions

After you have specified the COM+ Probe for the target COM+ Server, you use the Browse Counters Utility in the monitor configuration screen. The COM+ probe will be queried for a list of available functions to monitor, and a browse tree will be displayed. See the Browsable Counter Utility help page for instructions on how to navigate this hierarchy tree and select your functions or counters of interest.

Configuring the COM+ Server Monitor

The COM+ Server Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the COM+ Server Monitor.

Main Settings for the COM+ Server Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the COM+ server, how often this COM+ Server Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this COM+ Server monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the COM+ Server Monitor should system check the COM+ server. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

COM+ Probe Host Name

Enter the host name of the COM+ Probe.

COM+ Probe Port Number

Specify the port number of the COM+ Probe. The installation default for the probe is at port 8008.

Authorization User Name

Optional user name for authorization to the probe.

Authorization Password

Optional password for authorization to the probe.

HTTP Proxy

Optionally, a proxy server can be used to access the probe. Enter the domain name and port of an HTTP Proxy Server.

Proxy Server User Name

If the proxy server requires a name and password to access the probe, enter the name here. Your proxy server must support Proxy-Authenticate for these options to function.

Proxy Server Password

If the proxy server requires a name and password to access the probe, enter the password here.

Counters

You select the counters to be monitored by the COM+ Server Monitor using the expandable menu tree feature. The menu tree is automatically populated after you enter a valid address for the **COM+ Probe Host Name** and other connection properties and then click the **Get Counters** button. Use the selection features in the counters menu tree to expand or contract the counter tree and select the counters you want to monitor with this monitor instance.

Advanced Settings for the COM+ Server Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the COM+ Server Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Timeout

The number of seconds that the monitor should wait for a response from the server before timing-out. Once this time period passes, the monitor will log an error and report an error status.

Note: Depending on the activity on the server, the time to build the server monitor statistics Web page may take more than 15 seconds. You should test the monitor with an Timeout value of more than 60 seconds to allow the server to build and serve the server monitor statistics Web page before the SiteScope monitor is scheduled to run again.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set one or more status thresholds criteria for each status condition per monitor instance. The status of the monitor and any associated alert action will be set based on comparison of all the threshold criteria you define for the monitor. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the COM+ Server or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the COM+ Server Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

88

Exchange 2003 Mailbox Monitor

The Exchange 2003 Mailbox Monitor monitors mailbox statistics of Exchange Server 2003.

This chapter describes:	On page:
About the Exchange 2003 Mailbox Monitor	913
Editing the Exchange 2003 Mailbox Monitor	914

Note: The Exchange 2003 Mailbox Monitor is an optional SiteScope feature. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your Mercury sales representative for more information.

About the Exchange 2003 Mailbox Monitor

The Exchange 2003 Mailbox Monitor displays important statistics about mailboxes, including mailboxes that are over a certain size, and mailboxes that have not been accessed in some number of days.

About Scheduling This Monitor

This monitor computes statistics that do not normally change very rapidly and are not critical to system availability, so it should be scheduled to run infrequently, or on demand only. The results of each execution are saved and later viewable through the Usage Stats link.

Note: SiteScope must be configured to logon as a user account within the domain when running as a service, and not as "Local System account".

Editing the Exchange 2003 Mailbox Monitor

The Exchange 2003 Mailbox Monitor is part of the Exchange Solution. This monitor type can only be added by deploying an Exchange Solution template. Once the monitor has been created, you can edit the configuration of the monitor the same as other monitors. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the Exchange 2003 Mailbox Monitor.

Main Settings for the Exchange 2003 Mailbox Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the Exchange mailbox, how often this Exchange 2003 Mailbox Monitor instance should be run, and the text name used for this monitor instance. See “Common Monitor Settings” in the chapter “Working with SiteScope Monitors” for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this Exchange 2003 Mailbox monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the Exchange 2003 Mailbox Monitor should mailbox check the Exchange mailbox. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Server

Choose the server that you want to monitor. The server should be running Exchange Server 2003.

Username

Enter the username to use when querying the server for mailbox statistics. The statistics are gathered via WMI (Windows Management Instrumentation), so the username entered here must have permissions to read WMI statistics on the server from WMI namespace root\MicrosoftExchangeV2. If this field is left blank, the user that SiteScope is running as will be used.

Password

Enter the password for the username entered above, or blank if username is left blank.

Days since access

Enter the number of days (N) to use when reporting the number of mailboxes that have not been accessed in N days.

N largest mailboxes

Enter the number (N) of mailboxes to display when reporting the N largest mailboxes.

Advanced Settings for the Exchange 2003 Mailbox Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Exchange 2003 Mailbox Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Directory to write reports to

Enter a location for SiteScope to save the results of each execution of this monitor. A default location will be chosen if this field is left blank.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set up to ten status thresholds criteria for each status condition per monitor instance. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the Exchange 2003 Mailbox or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.

3 Enter a value applicable to the measurement parameter in the third text box.

4 To add another threshold setting, click the **New Error If** button and repeat the steps above.

5 Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the Exchange 2003 Mailbox Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

89

Exchange 2003 Public Folder Monitor

The Exchange 2003 Public Folder Monitor monitors public folder statistics of Exchange Server 2003.

This chapter describes:	On page:
About the Exchange 2003 Public Folder Monitor	921
Editing the Exchange 2003 Public Folder Monitor	922

Note: The Exchange 2003 Public Folder Monitor is an optional SiteScope feature. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your Mercury sales representative for more information.

About the Exchange 2003 Public Folder Monitor

The Exchange 2003 Public Folder Monitor displays statistics about public folders, such as access times, empty folders, folder sizes, and folders not accessed within some time period.

About Scheduling This Monitor

This monitor computes statistics that do not normally change very rapidly and are not critical to system availability, so it should be scheduled to run infrequently, or on demand only. The results of each execution are saved and later viewable through the Usage Stats link.

Note: SiteScope must be configured to logon as a user account within the domain when running as a service, and not as "Local System account".

Editing the Exchange 2003 Public Folder Monitor

The Exchange 2003 Public Folder Monitor is part of the Exchange Solution. This monitor type can only be added by deploying an Exchange Solution template. Once the monitor has been created, you can edit the configuration of the monitor the same as other monitors. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the Exchange 2003 Public Folder Monitor.

Main Settings for the Exchange 2003 Public Folder Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the Exchange Server Public Folder, how often this Exchange 2003 Public Folder Monitor instance should be run, and the text name used for this monitor instance. See “Common Monitor Settings” in the chapter “Working with SiteScope Monitors” for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this Exchange 2003 Public Folder monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the Exchange 2003 Public Folder Monitor should system check the Exchange Server Public Folder. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Server

Choose the server that you want to monitor. The server should be running Exchange Server 2003.

Username

Enter the username to use when querying the server for mailbox statistics. The statistics are gathered via WMI (Windows Management Instrumentation), so the username entered here must have permissions to read WMI statistics on the server from WMI namespace root\MicrosoftExchangeV2. If this field is left blank, the user that SiteScope is running as will be used.

Password

Enter the password for the username entered above, or blank if username is left blank.

Days since access

Enter the number of days (N) to use when reporting the number of public folders that have not been accessed in N days.

Advanced Settings for the Exchange 2003 Public Folder Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Exchange 2003 Public Folder Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Directory to write reports to

Enter a location for SiteScope to save the results of each execution of this monitor. A default location will be chosen if this field is left blank.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule

➤ Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set up to ten status thresholds criteria for each status condition per monitor instance. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the Exchange 2003 Public Folder or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the Exchange 2003 Public Folder Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

90

Exchange 2000/2003 Message Traffic Monitor

The Exchange 2000/2003 Message Traffic Monitor monitors message statistics of Exchange Server 2000/2003.

This chapter describes:	On page:
About the Exchange 2000/2003 Message Traffic Monitor	929
Editing the Exchange 2000/2003 Message Traffic Monitor	930

Note: The Exchange 2000/2003 Message Traffic Monitor is an optional SiteScope feature. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your Mercury sales representative for more information.

About the Exchange 2000/2003 Message Traffic Monitor

The Exchange 2000/2003 Message Traffic Monitor displays important statistics about messages handled by an Exchange 2000/2003 server, such as a count of messages sent that are larger than a certain size, or sent to a large number of recipients.

About Scheduling This Monitor

This monitor computes statistics that do not normally change very rapidly and are not critical to system availability, so it should be scheduled to run infrequently, or on demand only. The results of each execution are saved and later viewable through the Usage Stats link.

Note: SiteScope must be configured to logon as a user account within the domain when running as a service, and not as "Local System account".

Editing the Exchange 2000/2003 Message Traffic Monitor

The Exchange 2000/2003 Message Traffic Monitor is part of the Exchange Solution. This monitor type can only be added by deploying an Exchange Solution template. Once the monitor has been created, you can edit the configuration of the monitor the same as other monitors. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the Exchange 2000/2003 Message Traffic Monitor.

Main Settings for the Exchange 2000/2003 Message Traffic Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the Exchange server, how often this Exchange 2000/2003 Message Traffic Monitor instance should be run, and the text name used for this monitor instance. See “Common Monitor Settings” in the chapter “Working with SiteScope Monitors” for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this Exchange 2000/2003 Message Traffic monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the Exchange 2000/2003 Message Traffic Monitor should system check the Exchange server. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Server

Choose the server that you want to monitor. The server should be running Exchange Server 2000 or Exchange Server 2003.

Username

Enter the username to use when querying the server for mailbox statistics. The statistics are gathered via WMI (Windows Management Instrumentation), so the username entered here must have permissions to read WMI statistics on the server from WMI namespace root\MicrosoftExchangeV2. If this field is left blank, the user that SiteScope is running as will be used.

Password

Enter the password for the username entered above, or blank if username is left blank.

Query interval

Enter the number of minutes to look back for messages when computing statistics. This will affect how long it takes to execute the monitor as a large interval could result in a large number of messages to be processed.

Message size limit

Enter the number (N) of bytes to use when computing the number of messages sent larger than N bytes.

Recipient limit

Enter the number (N) of recipients to use when computing the number of messages sent to more than N recipients.

Number of domains

Enter the number (N) of domains to use for reporting the top N sending domains.

Number of outgoing users

Enter the number (N) of users to use for reporting the top N outgoing users.

Advanced Settings for the Exchange 2000/2003 Message Traffic Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Exchange 2000/2003 Message Traffic Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Directory to write reports to

Enter a location for SiteScope to save the results of each execution of this monitor. A default location will be chosen if this field is left blank.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set up to ten status thresholds criteria for each status condition per monitor instance. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the Exchange 2000/2003 Message Traffic or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the Exchange 2000/2003 Message Traffic Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

91

Exchange 5.5 Message Traffic Monitor

The Exchange 5.5 Message Traffic Monitor monitors message statistics of Exchange Server 5.5.

This chapter describes:	On page:
About the Exchange 5.5 Message Traffic Monitor	937
Editing the Exchange 5.5 Message Traffic Monitor	938

Note: The Exchange 5.5 Message Traffic Monitor is an optional SiteScope feature. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your Mercury sales representative for more information.

About the Exchange 5.5 Message Traffic Monitor

This Exchange 5.5 Message Traffic Monitor displays important statistics about messages handled by an Exchange 5.5 server, such as a count of messages sent that are larger than a certain size, or sent to a large number of recipients.

About Scheduling This Monitor

This monitor computes statistics that do not normally change very rapidly and are not critical to system availability, so it should be scheduled to run infrequently, or on demand only. The results of each execution are saved and later viewable through the Usage Stats link.

Editing the Exchange 5.5 Message Traffic Monitor

The Exchange 5.5 Message Traffic Monitor is part of the Exchange Solution. This monitor type can only be added by deploying an Exchange Solution template. Once the monitor has been created, you can edit the configuration of the monitor the same as other monitors. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the Exchange 5.5 Message Traffic Monitor.

Main Settings for the Exchange 5.5 Message Traffic Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the Exchange 5.5 server, how often this Exchange 5.5 Message Traffic Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this Exchange 5.5 Message Traffic monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the Exchange 5.5 Message Traffic Monitor should system check the Exchange 5.5 server. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Log directory

Enter a UNC path to the directory where message tracking logs are stored for the Exchange 5.5 server. Generally, this path will be \\<servername>\tracking.log

Query interval

Enter the number of minutes to look back for messages when computing statistics. This will affect how long it takes to execute the monitor as a large interval could result in a large number of messages to be processed.

Message size limit

Enter the number (N) of bytes to use when computing the number of messages sent larger than N bytes.

Recipient limit

Enter the number (N) of recipients to use when computing the number of messages sent to more than N recipients.

Number of domains

Enter the number (N) of domains to use for reporting the top N sending domains.

Number of outgoing users

Enter the number (N) of users to use for reporting the top N outgoing users.

Advanced Settings for the Exchange 5.5 Message Traffic Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Exchange 5.5 Message Traffic Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Directory to write reports to

Enter a location for SiteScope to save the results of each execution of this monitor. A default location will be chosen if this field is left blank.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule

➤ Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set up to ten status thresholds criteria for each status condition per monitor instance. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the Exchange 5.5 Message Traffic or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the Exchange 5.5 Message Traffic Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

92

SAP CCMS Monitor

The SAP CCMS Monitor allows you to monitor the performance of your SAP R/3 System landscape in a centralized manner using SAP's CCMS interface.

This chapter describes:	On page:
Understanding the SAP CCMS Monitor	945
SAP Java Connector Installation	947
Configuring the SAP CCMS Monitor	949

Note: The SAP CCMS Monitor is an optional SiteScope feature. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your Mercury sales representative for more information.

Understanding the SAP CCMS Monitor

The SAP CCMS Monitor retrieves and reports metrics using SAP's new centralized monitoring architecture, CCMS (Computer Center Management System). With CCMS, a SAP administrator can monitor all servers, components and resources in the R/3 landscape from a single centralized server, greatly facilitating not only problem discovery but also problem diagnosis.

Using SAP's advanced CCMS interface BC-XAL 1.0, the SiteScope SAP CCMS Monitor exposes hundreds of performance and availability metrics. The error and warning thresholds for the monitor can be set for one or more of the nearly 120 SAP server performance statistics available via the CCMS interface.

Note: Due to the large amount of metrics that are being retrieved when displaying the entire SAP metrics browse tree during monitor definition, there could be a noticeable delay going from the Choose Server page to the Choose Counters page (possibly 1 to 2 minutes). However, once a browse tree has been successfully retrieved it will be cached to file automatically, so that the next time you retrieve metrics from the same server/username the wait time will be greatly reduced.

This monitor only retrieves and displays numeric metrics (Performance attributes). That is, Status, Log and Information attributes are currently not supported. Also, presentation and management of SAP CCMS Alerts in SiteScope are not supported at this time.

The default run schedule for this monitor is every 10 minutes, but you can change it to run more or less often using the **Frequency** setting. Note, however, that CCMS metrics are generally only updated once every 5 minutes.

To enable the SAP CCMS monitor, you must install the SAP Java Connector. For details, see "SAP Java Connector Installation" on page 947.

Software Requirements

- The SAP CCMS Monitor requires that the SAP Java Connector (SAP JCo 2.0.6 and above) component be downloaded from the SAP Service Marketplace Software Distribution Center, and installed on the same server where SiteScope is running (or at least be accessible on a shared or remote location).
- The BC-XAL 1.0 interface is supported on R/3 systems 4.5B and above only.

➤ Consult your SAP documentation to determine if your R/3 landscape components may need additional software installed to run or work with CCMS.

To download SAP Java Connector, go to the SAP Software Distribution Center at:

http://www.service.sap.com/connectors

Then click "SAP Java Connector" and then click "Tools and Services".

Note: You will need a valid Service Marketplace login to access this SAP Web site.

User Authorization

A SAP user requires certain privileges to read CCMS metrics. When defining a SAP CCMS Monitor in SiteScope you must specify a user who has XMI authorization to be able to login to the CCMS server and retrieve metrics. The user should have one or more of the profiles listed below assigned to it. Authorizations are collected in SAP profiles, and the following profiles include XMI authorization:

➤ S_A.SYSTEM

➤ PD_CHICAGO

➤ S_WF_RWTEST

➤ SAP_ALL

One test to see if a user has such authorization is to try and issue transaction RZ20 in the SAP GUI and see if the CCMS monitor sets can be displayed.

SAP Java Connector Installation

The SAP CCMS monitor uses SAP JCo libraries to connect to the SAP R/3 system. A user must have the appropriate license granted by SAP to receive and use these libraries.

To enable the SAP CCMS monitor on a Windows environment:

1 Download the following .jar file and .dll files from the SAP support Web site:

- **sapjco.jar**
- **librfc32.dll**
- **sapjcorfc.dll**

2 Copy the **sapjco.jar** file into the **<SiteScope root directory>/WEB-INF/lib** directory.

3 Copy the two .dll files into the **<SiteScope root directory>/bin** directory.

Note: Check if the .dll files already exist in your **<Windows installation directory>/system32** directory. They may have been copied into this directory as part of the SAP client installation. If they do exist in your system, you must overwrite them with the above .dll files before copying into the SiteScope directory.

---

4 Restart SiteScope.

To enable the SAP CCMS monitor on a UNIX environment:

1 Download the following .jar file and .so files from the SAP support Web site:

- **sapjco.jar**
- **librfccm.so**
- **libsapjcorfc.so**

2 Copy the **sapjco.jar** file into the **<SiteScope root directory>/WEB-INF/lib** directory.

3 Copy the two .so files as follows:

- For Sun installations, copy into the **<SiteScope root directory>/java/bin/sparc** directory.
- For Linux installation, copy into the **<SiteScope root directory>/java/bin/i386** directory.

4 Restart SiteScope.

Configuring the SAP CCMS Monitor

The SAP CCMS Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the SAP CCMS Monitor.

Main Settings for the SAP CCMS Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the SAP server, how often this SAP CCMS Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this SAP CCMS monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the SAP CCMS Monitor should system check the SAP server. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Application Server

Enter the address of the SAP server you want to monitor.

SAP Client

Enter the Client to use for connecting to SAP.

System Number

Enter the System number for the SAP server.

Authorization User Name

Enter the user name required to connect to the SAP server.

Authorization Password

Enter the password required to connect to the SAP server.

SAP Router String

If your connection is being made through a router, enter a router address string. You can find the router address using the SAP Logon tool from the SAP Client software. Open the Logon console, select the server you want to monitor and then select **Properties** to view the router address. Leave it blank otherwise.

Counters

Choose the server performance parameters or counters you want to check with this monitor. Click **Get Counters** to bring up the counters selection screen where an expandable browse tree will be displayed. This tree will more or less match the hierarchy of Monitoring Tree Elements displayed in the Monitoring Tree that is shown in the SAP GUI with transaction RZ20. However, our browse tree may show more or less information than RZ20 depending on the authorization level of the username you specified for this monitor. Check or clear the check boxes on the Get Counters screen to select counters to monitor on this server.

Advanced Settings for the SAP CCMS Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the SAP CCMS Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set one or more status thresholds criteria for each status condition per monitor instance. The status of the monitor and any associated alert action will be set based on comparison of all the threshold criteria you define for the monitor. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the SAP CCMS or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the SAP CCMS Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

93

SAP CCMS Alerts Monitor

This chapter describes the SAP CCMS Alerts monitor that allows you to read and complete alerts from the SAP CCMS monitors:

This chapter describes:	On page:
Understanding the SAP CCMS Alerts Monitor	955
SAP Java Connector Installation	957
Configuring the SAP CCMS Alerts Monitor	958

Note: The SAP CCMS Alerts Monitor is an optional SiteScope feature. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your Mercury sales representative for more information.

Understanding the SAP CCMS Alerts Monitor

The SAP CCMS Alerts Monitor retrieves and reports alerts from the SAP CCMS monitors using SAP's centralized monitoring architecture: CCMS (Computer Center Management System). Using SAP's advanced CCMS interface BC-XAL 1.0, this new SiteScope monitor retrieves alerts.

The SAP CCMS Alerts Monitor allows you to monitor and complete alerts for various components of your R/3 landscape.

The default run schedule for this monitor is every 10 minutes, but you can change it to run more or less often using the **Update every** setting. Note, however, that CCMS metrics are generally only updated once every 5 minutes.

To enable the SAP CCMS Alerts monitor, you must install the SAP Java Connector. For details, see "SAP Java Connector Installation" on page 957.

Software Requirements

The SAP Java Connector (SAP JCo 2.0.6 and above) component must be downloaded from the SAP Service Marketplace Software Distribution Center, and installed on the same server where SiteScope is running (or at least be accessible on a shared or remote location).

To download SAP Java Connector, go to the SAP Software Distribution Center at: **http://www.service.sap.com/connectors**

Then click **SAP Java Connector**, **Tools and Services**. You will need a valid Service Marketplace login to access this site.

Note: The BC-XAL 1.0 interface is supported on R/3 systems 4.5B and above only.

Consult your SAP documentation to determine if your R/3 landscape components need additional software installed to run or work with CCMS.

User Authorization

A SAP user requires certain privileges to read CCMS metrics. When defining a SAP CCMS Alerts Monitor in SiteScope you must specify a user who has XMI authorization to be able to login to the CCMS server and retrieve metrics. The user should have one or more of the profiles listed below assigned to it. Authorizations are collected in SAP profiles, and the following profiles include XMI authorization:

- S_A.SYSTEM
- PD_CHICAGO
- S_WF_RWTEST

➤ SAP_ALL

One test to see if a user has such authorization is to try and issue transaction RZ20 in the SAP GUI and see if the CCMS monitor sets can be displayed.

SAP Java Connector Installation

The SAP CCMS Alerts monitor uses SAP JCo libraries to connect to the SAP R/3 system. A user must have the appropriate license granted by SAP to receive and use these libraries.

To enable the SAP CCMS Alerts monitor on a Windows environment:

1 Download the following .jar file and .dll files from the SAP support Web site:

- **sapjco.jar**
- **librfc32.dll**
- **sapjcorfc.dll**

2 Copy the **sapjco.jar** file into the <**SiteScope root directory**>/**WEB-INF/lib** directory.

3 Copy the two .dll files into the <**SiteScope root directory**>/**bin** directory.

Note: Check if the .dll files already exist in your <**Windows installation directory**>/**system32** directory. They may have been copied into this directory as part of the SAP client installation. If they do exist in your system, you must overwrite them with the above .dll files before copying into the SiteScope directory.

---

4 Restart SiteScope.

To enable the SAP CCMS Alerts monitor on a UNIX environment:

1 Download the following .jar file and .so files from the SAP support Web site:

- **sapjco.jar**
- **librfccm.so**

- **libsapjcorfc.so**

2. Copy the **sapjco.jar** file into the **<SiteScope root directory>/WEB-INF/lib** directory.
3. Copy the two .so files as follows:
   - For Sun installations, copy into the **<SiteScope root directory>/java/bin/sparc** directory.
   - For Linux installation, copy into the **<SiteScope root directory>/java/bin/i386** directory.
4. Restart SiteScope.

Configuring the SAP CCMS Alerts Monitor

The SAP CCMS Alerts Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the SAP CCMS Alerts Monitor.

Main Settings for the SAP CCMS Alerts Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the SAP R/3 system, how often this SAP CCMS Alerts Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this SAP CCMS Alerts monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the SAP CCMS Alerts Monitor should system performance check the SAP R/3 system. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Application Server

Enter the host name/IP address of the SAP server you want to monitor.

SAP Client

Enter the Client to use for connecting to SAP.

System Number

Enter the System number for the SAP server.

Authorization User Name

Enter the user name required to connect to the SAP server. This user must have authorization to access CCMS metrics; see the section on "User Authorization" for more information.

Authorization Password

Enter the Password required to connect to the SAP server.

SAP Router String

If your connection is being made through a router, enter a router address string. You can find the router address using the SAP Logon tool from the SAP Client software. Open the Logon console, select the server you want to monitor and then select Properties to view the router address. Leave it blank otherwise.

Counters

You use the features associated with the **Counters** setting to choose and manage the metrics you want to monitor with the SAP CCMS Alerts Monitor. Use the following steps to select and add counters.

To select or add counters:

1. Click **Get Counters** to query the remote system. After SiteScope has successfully connected to the remote system, the Get Counters selection dialogue opens.
2. Use the features in the Get Counters selection dialogue screen to select the SAP R/3 system metrics you want to monitor. Use the expandable menu controls as applicable to browse the available counters.
3. Use the check boxes to select between one and ten counters to be monitored.
4. Click **OK** to add the selected counters to the monitor configuration. The Get Counters selection dialogue closes and the monitor properties are updated with your selection.

Use the following steps to remove a counter from the selected counters list.

To remove or edit counters:

1. Click to edit the monitor for which you want to remove counters. Alternately, you may select the monitor you want to edit and click the Properties tab and click the **Edit** button. The monitor Properties screen opens.
2. Click the **Get Counters** button to open the Get Counters selection dialogue.
3. Clear the check box to the left of the current counter you want to remove.

   At this point, you may add other counters to the monitor by clicking the applicable check boxes.
4. Click **OK** at the bottom of the screen to update the monitor.

Advanced Settings for the SAP CCMS Alerts Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the SAP CCMS Alerts Monitor and its display in the product interface. See “Common Monitor Settings” in the chapter “Working with SiteScope Monitors” for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Thresholds Settings

You use the Threshold Settings section to set logic conditions that determine the status of this SAP CCMS Alerts Monitor instance based on the results returned by the system performance check.

Each SAP CCMS Alerts Monitor instance has three status settings:

- **Error if**
- **Warning if**
- **Good if**

You can set up to ten status thresholds conditions for each status settings per SAP CCMS Alerts Monitor instance. By default, only one threshold is displayed when you first configure the monitor.

While the monitor is enabled, it is assigned a status of good, warning, or error based on the most recent execution of the monitor action. The measurement taken or the results reported by the monitor are tested against the status threshold settings to determine the status.

The individual results are combined as logical OR relationships when more than one threshold condition is defined for any of the three settings. When one or more of the conditions (for example when two conditions for **Error if** setting) are met for a status setting the monitor status is set to the corresponding status condition. If status conditions are met for more than one status setting the status of the monitor is set to the highest valued status condition. For example, if one condition selected as Error if and another condition selected as Warning if are both met, the status would be reported as an error, with **error** being the highest value, **warning** the next highest and **good** the lowest value. The status is displayed by color and a status icon in the SiteScope interface.

A change of status signals an event and acts as a trigger for alerts associated with the monitor or the group to which the monitor belongs. For example, if the SAP CCMS Alerts Monitor detects that the SAP R/3 system has become unavailable, the status change from good to error is used to trigger an alert on error.

A change of status may also affect the state of a dependency between monitors. For example, a monitor that detects a change that results in a error status may be a trigger to disable one or more other monitors that are dependent on the SAP R/3 system.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement value. You may use the default status thresholds defined for the SAP CCMS Alerts Monitor or change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. In the SAP CCMS Alerts Monitor properties page, click **Threshold Settings** to open the Threshold Settings area:
2. Select **Error if** and select the measurement parameter you want to use to determine the error threshold in the appropriate boxes. To add the new threshold settings click **New Error If**.
3. Select **Warning if** and select the measurement parameter you want to use to determine the warning threshold in the appropriate boxes. To add the new threshold settings click **New Error If**.
4. Select **Good if** and select the measurement parameter you want to use to determine the good threshold in the appropriate boxes. To add the new threshold settings click **New Error If**.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the SAP CCMS Alerts Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

➤ Do not report to Mercury Business Availability Center

- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

94

SAP Java Web Application Server Monitor

The SAP Java Web Application Server Monitor allows you to monitor the availability and server statistics for SAP Java Web Application server cluster.

This chapter describes:	On page:
Understanding the SAP Java Web Application Server Monitor	967
SAP JMX Connector Installation	968
Configuring the SAP Java Web Application Server Monitor	968

Note: The SAP Java Web Application Server Monitor is an optional SiteScope feature. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your Mercury sales representative for more information.

Understanding the SAP Java Web Application Server Monitor

The SiteScope SAP Java Web Application Server monitor allows you to monitor the availability and server statistics for SAP Java Web Application server cluster. A Java cluster consists of one instance of Dispatcher per host, and one or more Servers. The monitor presents a counter tree for each dispatcher and server in the cluster.

The default run schedule for this monitor is every 10 minutes, but you can change it to run more or less often using the Frequency setting.

To enable the SAP Java Web Application Server monitor, you must install the SAP JMX Connector. For details, see below.

SAP JMX Connector Installation

The SAP Java Web Application Server monitor uses SAP JMX Connector libraries to connect to SAP J2EE cluster. A user must have the appropriate license granted by SAP to receive and use these libraries.

To enable the SAP Java Web Application Server monitor:

1. Rename the **logging.jar** file from the SAP Java Web Application server to **sap_logging.jar** so as not to overwrite the SiteScope **logging.jar** file.
2. Copy the following .jar files from the SAP Java Web Application server installation:
   - **admin.jar**
   - **com_sap_pj_jmx.jar**
   - **exception.jar**
   - **sap_logging.jar** (renamed from **logging.jar** in SAP library)
   - **jmx.jar**

   into the <**SiteScope root directory**>/**WEB-INF/lib** directory.
3. Restart SiteScope.

Configuring the SAP Java Web Application Server Monitor

The SAP Java Web Application Server Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the SAP Java Web Application Server Monitor.

Main Settings for the SAP Java Web Application Server Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the SAP server, how often this SAP Java Web Application Server Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this SAP Java Web Application Server monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the SAP Java Web Application Server Monitor should system check the SAP server. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Application Server

Enter the address of the SAP Java Web Application Server you want to monitor.

Port

Enter the port number of the SAP Java Web Application Server you want to monitor. The default value 50004 is often used.

Authorization User Name

Enter the Username required to connect to the SAP server.

Authorization Password

Enter the Password required to connect to the SAP server.

Counters

Choose the counters you want to check with this monitor. Click **Get Counters** to open the counters selection screen where an expandable browse tree is displayed. These counters are received dynamically from the JMX. Select or clear the check boxes on the Get Counters screen to select counters to monitor on this server.

Advanced Settings for the SAP Java Web Application Server Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the SAP Java Web Application Server Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set one or more status thresholds criteria for each status condition per monitor instance. The status of the monitor and any associated alert action will be set based on comparison of all the threshold criteria you define for the monitor. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the SAP Java Web Application Server or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the SAP Java Web Application Server Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

95

SAP Work Processes Monitor

The SAP Work Processes Monitor allows you to monitor the effectiveness of your SAP R/3 server configurations. The monitor provides statistical information on work process performance. This information allows you to estimate whether the SAP R/3 Server is efficiently using its resources.

This chapter describes:	On page:
Understanding the SAP Work Processes Monitor	975
SAP Java Connector Installation	977
Configuring the SAP Work Processes Monitor	978

Note: The SAP Work Processes Monitor is an optional SiteScope feature. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your Mercury sales representative for more information.

Understanding the SAP Work Processes Monitor

A SAP work process is a program that executes the R/3 application tasks. Each work process acts as a specialized system service. In terms of the operating system, a group of parallel work processes makes up the R/3 runtime system.

Every work process specializes in a particular task type: dialog, batch, update, enqueue, spool, message, or gateway. In client/server terms, a work process is a service, and the computing system running the particular service is known as a server. For example, if the system is providing only dialog services, this is a dialog server, although commonly referred to as an application server.

The dispatcher assigns tasks to the free work processes, making optimal use of system resources and balancing the system load. The dispatcher knows and distributes pending tasks according to the type of the defined processes. The difference among the various work processes affects only those tasks or special services that have been assigned to the work processes through the dispatching strategy.

Work Process Counters

The SAP Work Processes monitor retrieves the list of work processes for a specific R/3 or Work Processes group (Dialog, Background, etc.). The monitor's counters are divided into 6 groups:

- All WP
- Dialog WP
- Update WP
- Background WP
- Enqueue WP
- Spool WP

In each group, 7 counters are available:

- Total number of WP
- Number of WP in status Waiting
- Number of WP in status Running
- Number of WP in status Stopped
- Number of WP in another status (none of the above)
- Max CPU
- Max Memory

To enable the SAP Work Processes monitor, you must install the SAP Java Connector. For details, see below.

SAP Java Connector Installation

The SAP Work Processes monitor uses SAP JCo libraries to connect to the SAP R/3 system. A user must have the appropriate license granted by SAP to receive and use these libraries.

To enable the SAP Work Processes monitor on a Windows environment:

1. Download the following .jar file and .dll files from the SAP support Web site:
   - **sapjco.jar**
   - **librfc32.dll**
   - **sapjcorfc.dll**
2. Copy the **sapjco.jar** file into the **<SiteScope root directory>/WEB-INF/lib** directory.
3. Copy the two .dll files into the **<SiteScope root directory>/bin** directory.

Note: Check if the .dll files already exist in your **<Windows installation directory>/system32** directory. They may have been copied into this directory as part of the SAP client installation. If they do exist in your system, you must overwrite them with the above .dll files before copying into the SiteScope directory.

---

4. Restart SiteScope.

To enable the SAP Work Processes monitor on a UNIX environment:

1. Download the following .jar file and .so files from the SAP support Web site:
   - **sapjco.jar**
   - **librfccm.so**
   - **libsapjcorfc.so**

2 Copy the **sapjco.jar** file into the **<SiteScope root directory>/WEB-INF/lib** directory.

3 Copy the two .so files as follows:

- For Sun installations, copy into the **<SiteScope root directory>/java/bin/sparc** directory.
- For Linux installation, copy into the **<SiteScope root directory>/java/bin/i386** directory.

4 Restart SiteScope.

Configuring the SAP Work Processes Monitor

The SAP Work Processes Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the SAP Work Processes Monitor.

Main Settings for the SAP Work Processes Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the SAP server, how often this SAP Work Processes Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this SAP Work Processes monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the SAP Work Processes Monitor should system check the SAP server. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Application Server

Enter the address of the SAP server you want to monitor.

SAP Client

Enter the Client to use for connecting to SAP.

System Number

Enter the System number for the SAP server.

Authorization User Name

Enter the user name required to connect to the SAP server.

Authorization Password

Enter the password required to connect to the SAP server.

SAP Router String

If your connection is being made through a router, enter a router address string. You can find the router address using the SAP Logon tool from the SAP Client software. Open the Logon console, select the server you want to monitor and then select **Properties** to view the router address. Leave it blank otherwise.

Counters

Choose the server work process counters you want to check with this monitor. Click **Get Counters** to open the counters selection screen where an expandable browse tree is displayed. For details on available counters, see "Work Process Counters" on page 976. Select or clear the check boxes on the Get Counters screen to select counters to monitor on this server.

Advanced Settings for the SAP Work Processes Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the SAP Work Processes Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule

➤ Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set one or more status thresholds criteria for each status condition per monitor instance. The status of the monitor and any associated alert action will be set based on comparison of all the threshold criteria you define for the monitor. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the SAP Work Processes or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the SAP Work Processes Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

96

Siebel Log File Monitor

The Siebel Log File Monitor watches for log file entries added to a group of log files by looking for entries containing a specific event type or subtype.

This chapter describes:	On page:
About the Siebel Log File Monitor	985
Configuring the Siebel Log File Monitor	986

Note: The Siebel Log File Monitor is an optional SiteScope feature. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your Mercury sales representative for more information.

About the Siebel Log File Monitor

The Siebel Log File Monitor is useful for automatically scanning multiple log files for error information. With SiteScope doing this for you at set intervals, you can eliminate the need to scan the logs manually. In addition, you can be notified of warning conditions that you might have otherwise been unaware of until something more serious happened.

Each time the Siebel Log File Monitor runs, it examines only those log entries added since the last time it ran.

Each time that it runs this monitor, SiteScope starts from the point in the file where it stopped reading last time it ran. This insures that you are only notified of new entries and speeds the rate at which the monitor runs.

Note: This behavior can be overridden but is not recommended and should only be done for trouble-shooting purposes.

About Scheduling This Monitor

You can schedule your Siebel Log File Monitors to run as often as every 15 seconds. However, depending on the size of the log files, the total number of monitors you have running, and whether the **Search from Start** option is selected, the monitor may take a considerable amount of time to run. The default update schedule is every 10 minutes which may be reasonable in most cases.

Configuring the Siebel Log File Monitor

The Siebel Log File Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the Siebel Log File Monitor.

Main Settings for the Siebel Log File Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the Siebel log file system, how often this Siebel Log File Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this Siebel Log File monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the Siebel Log File Monitor should log file check the Siebel log file system. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Server

Select the server where the log files you want to monitor are located. **Note:** This monitor does not support UNIX servers at this time.

Log File Directory

Enter the pathname to the log directory you want to monitor.

To monitor log files on a remote Windows NT/2000 server through NetBIOS specify a UNC path to the remote directory. For example, `\\remoteserver\logFileDirectory`

Note: If you are using SSH as a connection method to the remote NT server you will need to select the **java library** and **ssh1** options for that remote.

File Name

Select the log files that you want to monitor. A regular expression must be used to specify multiple files. *However, be warned that selecting too many log files to monitor can significantly degrade overall SiteScope performance*. **Note:** The search is not recursive and will only match files listed within the log file directory.

Severity

Select the severity level of entries to consider for matching. Entries that have the correct event type/subtype **and** have an equal or greater severity will be matched, those with a lesser severity will be ignored.

Event Type

Select the matching event type or subtype. The monitor will report how many log entries were found of the specified type.

Log-Entry Content Match

Optionally, you may specify an additional text string or regular expression to further narrow down the matched log entries. This match expression is run against the content returned from the initial Severity and Event Type match. You use this option to find only those log entries with the selected severity an event type that meet this additional match criteria.

Search from Start

Select file checking option for this monitor instance. This setting controls what SiteScope will look for and how much of the target file will be checked each time that the monitor is run. The following table describes the options for this setting:

Checking Option	Description
Off	Check only newly added records, starting at the time that the monitor was created (not when the file was created). **This is the default behavior.**
On	Always check the contents of the whole file.

Note: Using this option may have undesired impact on SiteScope performance. Monitoring large numbers of log files with this option may use large amounts of memory and CPU time on the SiteScope server which can lead to other performance problems.

Advanced Settings for the Siebel Log File Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Siebel Log File Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set up to ten status thresholds criteria for each status condition per monitor instance. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the Siebel Log File or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.

3 Enter a value applicable to the measurement parameter in the third text box.

4 To add another threshold setting, click the **New Error If** button and repeat the steps above.

5 Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the Siebel Log File Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

97

Siebel Application Server Monitor

The Siebel Application Server Monitor (previously know as the Siebel Server Manager Monitor) uses the Siebel Server Manager client to monitor Object Manager components and task information on Siebel application servers.

This chapter describes:	On page:
About the Siebel Application Server Monitor	995
Configuring the Siebel Application Server Monitor	998

Note: The Siebel Application Server Monitor is an optional SiteScope feature. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your Mercury sales representative for more information.

About the Siebel Application Server Monitor

The following are several key requirements for using the Siebel Application Server Monitor:

1 The Siebel Server Manager client must be installed on the machine where SiteScope is running or accessible to the SiteScope machine. There are several options for how you can do this:

➤ Copy the necessary client libraries from the Siebel server and install them on the machine where SiteScope is running (recommended option).

- ➤ Enable the client on the Siebel server itself and create a remote server profile in SiteScope to access that server and the Siebel client on that server.
- ➤ Install and enable the client on a third remote server and create a remote server profile in SiteScope to access that server and the Siebel client on that server.
- ➤ For Windows networks, map the network drive where the Siebel client is installed to the SiteScope machine and use this in the Script Path.

2 You will need to know the install path for the Server Manager client to be able to setup Siebel Server Manager monitors in SiteScope. If the client is installed on the machine where SiteScope is running, this will be the path on that machine. If the client is installed on a remote machine, you need to know the fully qualified path to the client executable relative to that machine.

3 You need to know the name of the Siebel application(s) that are available in your network. For example, callcenter, sales, and so forth.

4 You need to know the name or address of the Siebel Gateway server used by the Siebel applications you want to monitor. Ask your Siebel system administrator or consult the Siebel documentation for more information about the Gateway server name.

5 You need to know the name or address of the Siebel Enterprise server used by the Siebel applications you want to monitor. Ask your Siebel system administrator or consult the Siebel documentation for more information.

6 You need to know the user and password that SiteScope will use for logging into the Siebel server. This user must be granted Siebel Administrator responsibility on the Siebel server.

7 For monitoring Siebel processes, SiteScope will need credentials/authorization to access the target Siebel machine. You might need to define a Remote host in SiteScope for the target Siebel machine, unless the SiteScope server is already implicitly authenticated by the Siebel machine.

Note: Process monitoring remote Siebel machines incurs a noticeable delay (to get process metrics) hence the monitor will run slower than if the target Siebel machine is in close proximity to the SiteScope server. If your process counters are returning with no values during a run, it might be that the process metrics read operation is taking too long and SiteScope is timing out. In this case you might want to specify an appropriate timeout value for perfex in master.config (in seconds), for example: _perfexTimeout=120

---

8 You need to know the full path to the executable directory of the Siebel Server Manager Client relative to the machine it is installed on.

9 You need to make sure that the Siebel Server Manager Client's libraries are available to the Client. This will vary according to the platform on which SiteScope is running:

For SiteScope on UNIX/Linux - If the client libraries are installed locally, you will need to explicitly configure the LD_LIBRARY_PATH to include the directory containing the Siebel Server Manager Client's libraries (for example, /var/siebel/client/lib). If you are running the Siebel Server Manager Client locally on the SiteScope server, update the LD_LIBRARY_PATH line in the start-monitor script in the <SiteScope install path>/SiteScope/classes directory.

If you are accessing the Siebel Server Manager Client on a remote server, you will need to have a remote UNIX server profile to connect to that server. You will need to set the LD_LIBRARY_PATH on that machine by using the Initialize Shell Environment field for the remote server configuration created in SiteScope. An example shell initialization command would look like the following:

```
LD_LIBRARY_PATH=/var/siebel/client/lib;export LD_LIBRARY_PATH
```

For SiteScope on Windows - If the client libraries are installed locally, you need to add a system variable called LD_LIBRARY_PATH that includes the path to the bin directory of the Siebel Client Manager.

If you are accessing the Siebel Server Manager Client on a remote server, you will need to have a remote NT server profile to connect to that server (NetBIOS connections ONLY). You will need to enter the full path to the

Siebel Server Manager executable directory relative to the server chosen in the Script Path field on the Choose Server screen.

Configuring the Siebel Application Server Monitor

The Siebel Application Server Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the Siebel Application Server Monitor.

Main Settings for the Siebel Application Server Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the Siebel server, how often this Siebel Application Server Monitor instance should be run, and the text name used for this monitor instance. See “Common Monitor Settings” in the chapter “Working with SiteScope Monitors” for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this Siebel Application Server monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the Siebel Application Server Monitor should Siebel system check the Siebel server. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Server

Select or enter the remote Windows or UNIX machine where the Server Manager (srvrmgr) script is installed. The method of connection is either SSH or Telnet (but not Microsoft NetBios). For NetBios choose "this server" and map the drive.

Siebel Host Name

This field is required if you are doing either of the following:

- Doing process monitoring: In this case you must define a Remote Definition to the target Siebel machine whose Siebel processes are to be monitored. Then specify in this field the *Host Server Name* of the Siebel Remote definition (NOT the *Title*). This is the "NT Server Address" field for NT Remotes and "Server Address" field for Unix Remotes.
- Reporting monitor data to an installation of Mercury Business Availability Center: In this case the value entered will be used as a text identifier describing the target Siebel server that this monitor is monitoring. This text descriptor is used to identify the Siebel server when the monitor data is viewed in an Mercury Business Availability Center report. In this case the field is optional only if the Script Server field is already specified to be the target Siebel server

Application Server

Enter the Siebel server name or address.

Gateway Server

Enter the Gateway server name or address.

Enterprise Server

Enter the Enterprise server name or address.

Username

Enter the username for the Siebel Server Manager client.

Password

Enter the password for the Siebel Server Manager client.

Script Path

The full path to the Siebel Server Manager executable directory relative to the machine chosen above. For example, E:\sea704\client\BIN

Counters

Click **Get Counters** to choose the Siebel server statistics to be used as counters. The Get Counters page presents the counters available in an expandable tree format. Use the plus sign or minus sign features to expand or collapse the tree. Click the check box next to the counters you want to monitor. You can to select one or more counters to monitor with a single monitor instance. The following are typical of the counters available for the Siebel Server Manager Monitor:

- Server Stats/SiteScopeMSP/Avg SQL Execute Time
- Server Stats/SiteScopeMSP/Total Tasks
- Server Stats/SiteScopeMSP/Number of SQL Executes
- Server Stats/SiteScopeMSP/CPU Time
- Server Stats/SiteScopeMSP/Average Response Time
- Server Stats/SiteScopeMSP/Average Connect Time
- Server Stats/SiteScopeMSP/Total Response Time
- Component Stats/Business Integration Batch Manager/Elapsed Time
- Component Stats/Business Integration Batch Manager/CPU Time
- Component Stats/Business Integration Batch Manager/Number of SQL Executes
- Component Objects/Call Center Object Manager/CP_NUM_RUN
- Component Objects/Call Center Object Manager/CP_MAX_TASK

Advanced Settings for the Siebel Application Server Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Siebel Application Server Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Timeout

Enter the total time, in seconds, to wait for a successful test run. The time, in seconds, to wait for a success test run. After the defined timeout the monitor will stop running with an error timeout, and the browser and all the other processes created by running the monitor will be killed.

Detailed errors logging

Check this box if you want SiteScope to include detailed errors in the state string and in the log file in case of failure. In any case of failure, SiteScope will keep the log file of all the script execution, and a link to this log file will be available from the state string of the monitor and from the reports for future reference.

Process HTTP failure as error

Check this box if you want SiteScope to process every HTTP error (such as server not found) as an error in the monitor run. Note that choosing this option will fail the monitor and the transaction in which it appeared, even if a single .gif file is missing. By default HTTP errors counts as warning.

Process Checkpoint failure as warning

Check this box if you want SiteScope to process checkpoint failure as an error. Checkpoints are verification points that can be added using the ALT Recorder, and enable you to verify the content of a page. By default checkpoint failures are counted as errors.

Ignore warnings

Check this box if you want SiteScope to ignore all warnings appeared during the script execution. Note that choosing this option will cause all the Warnings thresholds to be ignored. By default SiteScope does not ignore warnings.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set one or more status thresholds criteria for each status condition per monitor instance. The status of the monitor and any associated alert action will be set based on comparison of all the threshold criteria you define for the monitor. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the Siebel Application Server or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the Siebel Application Server Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

98

Siebel Web Server Monitor

The Siebel Web Server Monitor allows you to use SiteScope to monitor statistical and operational information about a Siebel server by way of the Siebel Web server plug-in. You can use this monitor to watch Siebel server login session statistics and gauge the performance of the Siebel server Object Managers and database.

This chapter describes:	On page:
About the Siebel Web Server Monitor	1007
Configuring the Siebel Web Server Monitor	1008

Note: The Siebel Web Server Monitor is an optional SiteScope feature. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your Mercury sales representative for more information.

About the Siebel Web Server Monitor

The following are several key requirements for using the Siebel Web Server Monitor:

1. The Siebel Web server plug-in must be installed.
2. The Siebel Web server plug-in should be configured to enable the display of the statistics you want to monitor. This may require that stats page sections be enabled by editing the eapps.cfg file for the Siebel server. Consult the Siebel documentation for more information.

Configuring the Siebel Web Server Monitor

The Siebel Web Server Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the Siebel Web Server Monitor.

Main Settings for the Siebel Web Server Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the Siebel server, how often this Siebel Web Server Monitor instance should be run, and the text name used for this monitor instance. See “Common Monitor Settings” in the chapter “Working with SiteScope Monitors” for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this Siebel Web Server monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the Siebel Web Server Monitor should Siebel system check the Siebel server. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Server

Enter the URL of the Web plug-in server stats page for the application you want to monitor. For example, http://siebelsrv/service/_stats.swe. If the Siebel Web server is configured to support verbose mode, you can also use http://siebelsrv/service/_stats.swe?verbose=high to include information on "Locks" and "Current Operations Processing" for the Siebel server.

Password

Enter the password for accessing the Web server stats page.

Username

Enter the username to access the Web server stats page.

HTTP Proxy

If you are using a proxy to access the Siebel server, enter the proxy server to use including port (for example, proxy.sitescope.com:8080)

Proxy Server User Name

Enter the proxy user name if the proxy server requires authorization

Proxy Server Password

Enter the proxy password if the proxy server requires authorization

If access to the Siebel Web Server site is controlled by a centralized authorization and authentication access control system, the following fields are used to submit information to a HTML/CGI enabled authentication system. You can determine if authentication is required by trying to access the Web plug-in server stats page using a Web browser outside of SiteScope. If an HTML-based authentication form opens before you see the Siebel service statistics page, you will need to use the following fields to access the Siebel Webserver plug-in.

Authorization Form Name

When using HTML Form-based Authentication, this is the identifier of the authentication form within the Web page. The identifier is a number representing the place or order of the forms on an HTML page. For example, [1] is the first HTML <FORM> set, [2] is the second, and so forth. The default is [1] which assumes that the authentication information is entered into the first HTML <FORM> tag set on the page.

Authorization Username Form Field

When using HTML Form-based Authentication, enter the username that should be submitted to the access control system. This must be the username that would be entered in the authentication form the same as if you were accessing the Siebel Web server plug-in manually using a Web browser.

Authorization Password Form Field

Enter the password that should be submitted to the access control system. This must be the password that would be entered in the authentication form when accessing the Siebel Web server plug-in manually using a Web browser.

Authorization Form Button

When using HTML Form-based Authentication, this is the identifier of the Submit button on the authentication form. The identifier is a number representing the place or order of the buttons on an HTML page. For example, [1] is the first HTML <INPUT TYPE=SUBMIT> button, [2] is the second, and so forth. The default is [1] which assumes that the form Submit button is the first Submit button.

Counters

You select the counters to be monitored by the Siebel Web Server Monitor using the expandable menu tree feature. The menu tree is automatically populated after you enter a valid connection properties and then click the **Get Counters** button. Use the selection features in the counters menu tree to expand or contract the counter tree and select the counters you want to monitor with this monitor instance. The following are typical of the counters available for the Siebel Web Server Monitor:

System Stats	**Applications (typical)**
Anonymous sessions requested from the pool • Value • General Stats count • General Stats mean • General Stats stddev • Frequency mean • Frequency stddev	/sales/Session Lifespan • Value • General Stats count • General Stats mean • General • Stats stddev • Frequency mean • Frequency stddev
Open Session Time • Value • General Stats count • General Stats mean • General Stats stddev • Frequency mean • Frequency stddev	/sales/ • Value • General Stats count • General Stats mean • General • Stats stddev • Frequency mean • Frequency stddev

Anon Session Available • Value • General Stats count • General Stats mean • General Stats stddev • Frequency mean • Frequency stddev	/callcenter/ • Value • General Stats count • General Stats mean • General • Stats stddev • Frequency mean • Frequency stddev
Close Session Time • Value • General Stats count • General Stats mean • General Stats stddev • Frequency mean • Frequency stddev	/callcenter/Session Lifespan • Value • General Stats count • General Stats mean • General • Stats stddev • Frequency mean • Frequency stddev
Request Time • Value • General Stats count • General Stats mean • General Stats stddev • Frequency mean • Frequency stddev	
Anon Session Removed • Value • General Stats count • General Stats mean • General Stats stddev • Frequency mean • Frequency stddev	

Response Time • Value • General Stats count • General Stats mean • General Stats stddev • Frequency mean • Frequency stddev	
Anonymous sessions returns to the pool • Value • General Stats count • General Stats mean • General Stats stddev • Frequency mean • Frequency stddev	

Advanced Settings for the Siebel Web Server Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Siebel Web Server Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Timeout

Enter the total time, in seconds, to wait for a successful test run. The time, in seconds, to wait for a success test run. After the defined timeout the monitor will stop running with an error timeout, and the browser and all the other processes created by running the monitor will be killed.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule

➤ Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set one or more status thresholds criteria for each status condition per monitor instance. The status of the monitor and any associated alert action will be set based on comparison of all the threshold criteria you define for the monitor. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the Siebel Web Server or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the Siebel Web Server Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

99

WebSphere MQ Status Monitor

The WebSphere MQ Status Monitor allows you to monitor the performance attributes of MQ Objects: channels and queues, on MQ Servers v5.2 and above (formerly known as MQSeries). Both performance attributes and events for channels and queues can be monitored.

This chapter describes:	On page:
About the WebSphere MQ Status Monitor	1019
Software Prerequisites	1020
List of Available Metrics	1020
Channel Status Codes	1021
Monitoring MQ Events	1022
Authentication	1024
Configuring the WebSphere MQ Status Monitor	1024

Note: The WebSphere MQ Status Monitor is an optional SiteScope feature. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your Mercury sales representative for more information.

About the WebSphere MQ Status Monitor

The error and warning thresholds for the WebSphere MQ Status Monitor can be set on as many as fifteen function measurements.

The default run schedule for this monitor is every 10 minutes, but you can change it to run more or less often using the **Frequency** setting.

Software Prerequisites

This monitor requires two IBM MQ SupportPacs to be downloaded from the IBM Web site and installed on the same machine where the SiteScope server is running:

- MA88: MQSeries classes for Java, version 5.2.2 (5648-C60) or later. Go to the IBM Web site for this support package. Note that in some cases this component may already be bundled with the IBM MQ Server installation. Check your IBM MQ install documentation for details.
- MS0B: WebSphere MQ Java classes for PCF. Go to the IBM Web site for this support package.

Follow the instructions for installing both support packs. Then copy the following files from these installations to **<SiteScope install path>\SiteScope\java\lib\ext** directory:

com.ibm.mq.jar

com.ibm.mq.pcf.jar

connector.jar

After installing the required libraries, stop and restart SiteScope.

List of Available Metrics

The following performance attributes and events for **queues** can be monitored:

- Current Queue Depth
- Queue Open Input Count
- Queue Open Output Count
- Event: Queue Depth High

- Event: Queue Depth Low
- Event: Queue Full
- Event: Queue Service Interval High
- Event: Queue Service Interval OK

The following performance attributes and events for **channels** can be monitored:

- Channel Status
- Channel Time Between Sends
- Channel Messages Transferred
- Channel Bytes Sent
- Channel Bytes Received
- Channel Buffers Sent
- Channel Buffers Received
- Event: Channel Activated
- Event: Channel Not Activated
- Event: Channel Started
- Event: Channel Stopped
- Event: Channel Stopped by User

Channel Status Codes

You can choose from two different reporting schemes for Channel Status Code values:

- IBM MQ Native Coding Scheme - report the actual or original channel status codes as documented in the IBM MQ literature.

➤ Mercury Coding Scheme - report channel status codes in ascending values that are directly proportional to the health of the channel. That is, SiteScope will report a channel status value from 0 (least healthy) to 6 (healthiest). This scheme is consistent with how other Mercury products report MQ channel status codes. However this scheme provides less gradients than the IBM scheme, as shown in the table below:

MQ Channel Status	MQ Coding Scheme	Mercury Coding Scheme
Stopped	6	0
Paused	8	0
Inactive	-1	0
Initializing	4	1
Stopping	13	1
Starting	2	2
Retrying	5	3
Requesting	7	4
Binding	1	5
Running	3	6

You can select the desired coding scheme in the "Channel Status Code Scheme" field under the Advanced Settings section.

Monitoring MQ Events

For events, two system queues are regularly polled for the presence of relevant events:

➤ SYSTEM.ADMIN.PERFM.EVENT - for queue performance events

➤ SYSTEM.ADMIN.CHANNEL.EVENT - for channel events

On each scheduled run of the MQ monitor (which contain event counters), one or both of these system queues are queried for the presence of events that match the chosen event type, the source queue or channel that generated the event, and its queue manager. Events found are only browsed and not removed from the queue, so such events can continue to be consumed by other applications, if necessary. On each run the MQ monitor will report the number of event occurrences found since the last run of the monitor.

The monitor will strive to not report the same event occurrence more than once. This is accomplished by recording the timestamp of the most recent event browsed, so that in the next monitor run any events encountered that were generated prior to this recorded timestamp will be ignored.

Enabling Queue Events on the MQ Server

By default queue performance events are disabled in the MQ server. In order for SiteScope to monitor these events you must enable the MQ server to generate these events. A MQSC command must be issued on each queue and for each event to be enabled. In addition, appropriate threshold values must be set on each queue and for each event, that specify the conditions for generating the event. Consult the IBM MQ MQSC Command Reference for more information. On the other hand, channel events are always enabled and require no further action for them to operate.

Specifying Alternate Queue Managers

It is possible to set up an MQSeries environment such that events from remote queue managers are routed to a central queue manager for monitoring. If the event configured for monitoring by the user is from a remote queue manager (a queue manager other than the one identified in the **Queue Manager** box of the MQ Monitor definition page), it must be specified in the **Alternate Queue Manager** box.

Authentication

Your MQ server may require SiteScope to authenticate itself when connecting to retrieve metrics. For this reason a feature has been built into this monitor to invoke a user-developed, client-side security exit written in Java. Do this by specifying the fully-qualified class name of the security exit component in file SiteScope\groups\master.config, as follows:

_mqMonitorSecurityExit=com.mycompany.mq.MyExit

where, in this example, your security exit class is called "com.mycompany.mq.MyExit". Make sure this class is in the classpath of the running SiteScope JVM. One way of accomplishing this is to copy your security exit class into the **<SiteScope install path>\SiteScope\java\lib\ext** directory. Note that you can only deploy one security exit class for a SiteScope instance, and every MQ monitor running on that instance will invoke that security exit.

In the case of a Windows-based SiteScope instance monitoring a Windows-based MQ server, the default authentication scheme requires that SiteScope be running under a user account that is recognized by the target server's Windows security group. Specifically, the SiteScope user must be added to the server's mqm group.

For information on MQ security exits and other authentication schemes consult the IBM WebSphere MQ documentation.

Configuring the WebSphere MQ Status Monitor

The WebSphere MQ Status Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the WebSphere MQ Status Monitor.

Complete the items on the Add MQ Status Monitor Form as follows. First you need to specify details of the target MQ server that will be monitored, then click the *Select Measurements* link. There you will choose attributes (counters) of specified queues and/or channels to monitor. When you have completed your counter selections, click the **Add** Monitor button.

Main Settings for the WebSphere MQ Status Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the WebSphere MQ system, how often this WebSphere MQ Status Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this WebSphere MQ Status monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the WebSphere MQ Status Monitor should system check the WebSphere MQ system. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

MQ Server Name

Specify the host name of the MQ Server you want to monitor. Enter the network name of the server or the IP address of the server. For example, mqmachinename.

MQ Server Port

Specify the port number of the target MQ Server. The installation default port is 1414.

Server Connection Channel

Enter the name of the server connection channel of the target MQ server. Check with the MQ Server administrator for the name syntax of the server connection channel

Queue Manager

Enter the name of the queue manager whose queues or channels will be monitored.

Alternate Queue Manager

You can optionally enter an alternate queue manager name that has been set up to forward its events to the primary queue manager specified above (if you are interested in monitoring such forwarded events also).

Selected Measurements

Lists measurements that you have chosen, if any. The **Select Measurements** link allows you to add or delete counters for the monitor. Click this link after you have specified all the server information above.

Selecting Measurements

The Measurement Selection page is accessed by clicking on the *Select Measurements* link of the main MQ Monitor definition page. There are two primary window panes on this page:

- **Available Measurements:** A browse window which displays available MQ queue instances and channel instances, and counters to choose from. You must first select either Queue or Channel Objects to work with, in the **Objects:** drop down box. Once an object is selected, a connection to the MQ server will be made, using the server information provided in the previous page. A list of available queues or channels will be displayed, both system and user instances, depending on the object type selected. Upon pressing the **Add** button, any number of instances and counters you select via check boxes will be combined into individual monitoring counters, and listed in the *Selected Measurements* window, below.
- **Selected Measurements:** Lists the counters you have selected to be monitored from pressing the Add button. The "X" box preceding each counter allows you to delete the counter.

Advanced Settings for the WebSphere MQ Status Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the WebSphere MQ Status Monitor and its display in the product interface. See “Common Monitor Settings” in the chapter “Working with SiteScope Monitors” for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Timeout

The number of seconds that the monitor should wait for a response from the server before timing-out. Once this time period passes, the monitor will log an error and report an error status.

Note: Depending on the activity on the server, the time to build the server monitor statistics Web page may take more than 15 seconds. You should test the monitor with an Timeout value of more than 60 seconds to allow the server time to build and serve the server monitor statistics Web page before the SiteScope monitor is scheduled to run again.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set one or more status thresholds criteria for each status condition per monitor instance. The status of the monitor and any associated alert action will be set based on comparison of all the threshold criteria you define for the monitor. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the WebSphere MQ Status or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the WebSphere MQ Status Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

100

Browsable Windows Performance Counter Monitor

The Browsable Windows Performance Counter Monitor tracks the values of Windows performance statistics. These are the same statistics that can be viewed using the "Performance Monitor" application under Windows. This monitor is only available on the Windows version of SiteScope.

This chapter describes:	On page:
About the Browsable Windows Performance Counter Monitor	1034
Editing the Browsable Windows Performance Counter Monitor	1034

Note: The Browsable Windows Performance Counter Monitor is currently an optional SiteScope feature. Additional licensing may be required to enable this monitor type in the SiteScope interface. Contact you Mercury sales representative for more information.

About the Browsable Windows Performance Counter Monitor

Each time the Browsable Windows Performance Counter Monitor runs, it returns readings and a status message and writes them in the monitoring log file. The status is displayed in the group detail table for the monitor which represents the current value returned by this monitor. For example, 1.24 Interrupts/sec. The status is logged as either OK or warning. A count of the number of counters that could not be read is also kept, and error conditions can be created depending upon this count.

Editing the Browsable Windows Performance Counter Monitor

The Browsable Windows Performance Counter Monitor is part of the Solution template or SiteScope Health. This monitor type can only be added by deploying an Solution template or SiteScope Health template. Once the monitor has been created, you can edit the configuration of the monitor the same as other monitors. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the Browsable Windows Performance Counter Monitor.

Main Settings for the Browsable Windows Performance Counter Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the system, how often this Browsable Windows Performance Counter Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this Browsable Windows Performance Counter monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the Browsable Windows Performance Counter Monitor should system check the system. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Counter File

Choose the file that contains a list of counters from which to choose to monitor. Use the drop-down list to select a server from the list of remote servers that are available to the SiteScope agent.

The files in this list all reside in the <SiteScope install path>/SiteScope/templates.perfmon/browsable directory under SiteScope. There are a number of default files in the standard SiteScope distribution.

Server

Choose the server where the performance counters you want to monitor are found. Use the drop-down list to select a server from the list of remote servers that are available to the SiteScope agent.

Counters

Select the counters to monitor. Click **Get Counters** to change the selected counters.

Advanced Settings for the Browsable Windows Performance Counter Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Browsable Windows Performance Counter Monitor and its display in the product interface. See “Common Monitor Settings” in the chapter “Working with SiteScope Monitors” for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule

➤ Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set up to ten status thresholds criteria for each status condition per monitor instance. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the Browsable Windows Performance Counter or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the Browsable Windows Performance Counter Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

Part V

Integration Monitors

101

Working with SiteScope Integration Monitors

Integration Monitors enable you to capture and forward data from several Enterprise Management Systems (EMS) applications and servers into Mercury Business Availability Center.

This chapter describes:	On page:
Integration Monitor Overview	1043
Licensing	1045
Important Upgrade Information	1045
Integration Monitor Logging Options	1046
Troubleshooting Integration Monitors	1047

Integration Monitor Overview

Integration Monitors are run by the SiteScope data collector and are used to integrate data from third-party applications (typically EMS systems) into Mercury Business Availability Center.

This section includes the following topics:

- Integration Monitor Categories
- Configuration File Template Types

Integration Monitor Categories

Integration monitors can be divided into two categories:

- Integration monitors designed for use with specific EMS applications
- Technology Integration Monitors (generic monitors) designed for use with most EMS applications that support extraction of data from a database, log file or SNMP trap interface

Configuration File Template Types

To correctly map the data they collect to a format recognizable by Mercury Business Availability Center , Integration Monitors use configuration files that you configure and customize as required. There are two types of configuration file templates:

- **Metrics data template** – Used to collect time-based data. Data collected by Integration Monitors that use the metrics data template (indicated with the term "metric" or "measurement" in the monitor name) is integrated into Mercury Business Availability Center as typical "SiteScope data" and can be viewed in all contexts that support viewing SiteScope data (for example, Dashboard, Service Level Management, System Availability Management , user reports, and so forth).
- **Event data template** – Used to collect data on specific events. Data collected by Integration Monitors that use the event data template (indicated with the term "event" or "ticket" in the monitor name) is integrated into Mercury Business Availability Center using the UDX framework and can be viewed in contexts that support the display of UDX data (Event Log, Dashboard, trend reports). The data can also be accessed using the Mercury Business Availability Center API.

Each specific Integration Monitor is designed to work with one of the templates. The Database , Log File, and SNMP Trap Technology Integration Monitors can be configured to work with either template. You use the configuration file templates that come prepackaged with SiteScope as a basis for creating a customized configuration file appropriate for your specific environment. When you configure an Integration Monitor in Monitor Administration, you point the monitor to the customized configuration file.

For details on customizing the Integration Monitor configuration file templates, see "Integration Monitor Configuration Files" on page 1049.

Licensing

Access to Integration Monitor types requires that a special SiteScope Optional License be entered on the SiteScope server. Several of these Integration Monitor types also require integration with another Mercury Interactive product or require additional software modules. Contact your Mercury Interactive sales representative for more information on the requirements for the Integration Monitors.

Note: It is highly recommended that all Integration Monitors be added into SiteScope groups specifically created to contain only Integration Monitors and no other monitor types.

Important Upgrade Information

Beginning with SiteScope 8.1, the monitor configuration file **main.config** is no longer used. All features that were supported in main.config are now supported in event.config.

Monitors from previous versions which have been customized by editing main.config can still be used although users are strongly encouraged to use event.config instead.

To use main.config for customized monitors from previous versions:

1. Copy or rename your customized **main.config** file to the SiteScope 8.1 directory. For details on working with integration configuration files, see "Integration Monitor Configuration Files" in *Configuring SiteScope Monitors*.
2. Change the directory path of each customized monitor to point to the SiteScope 8.1 directory.
   - ➤ In the monitor tree in SiteScope, right-click each monitor to edit that monitor. In the Main Settings area for each monitor, change the **EMS Configuration File Path** field to the new directory path. This new path must be identical to the directory path into which the main.config file was copied in step 1.

Integration Monitor Logging Options

Integration Monitor activity is logged to the following location:

<SiteScope root directory>\logs\EmsMonitors.log

You can modify the level and type of information reported to the log file by changing the log file settings in the <SiteScope root directory>\conf\log4j.properties file. You can instruct the logging mechanism to:

- report logged information in less or greater detail than is reported by default
- log all samples sent by Integration Monitors to Mercury Business Availability Center
- log all received events from external EMS systems

To modify log settings:

1. Open the log4j.properties file in a text editor.
2. To modify the level of logged information:
   - Locate the following lines in the file:

     log4j.category.com.mercury.sitescope.ems=${emsloglevel}, ems.appender
     log4j.additivity.com.mercury.sitescope.ems=false

   - Modify the argument of the log4j.category.com.mercury.sitescope.ems parameter from ${emsloglevel} to DEBUG, as follows:
     log4j.category.com.mercury.sitescope.ems=DEBUG, ems.appender

   You do not have to restart after making changes to the log4j file.
3. To specify that samples sent by Integration Monitors to Mercury Business Availability Center be logged:
   - Locate the following lines in the file:

     # Change ${emsloglevel} to DEBUG to see samples
     log4j.category.EmsSamplePrinter=${emsloglevel}, ems.appender
     log4j.additivity.EmsSamplePrinter=false

➤ Change the argument of the log4j.category.EmsSamplePrinter parameter from ${emsloglevel} to DEBUG, as follows:

```
log4j.category.EmsSamplePrinter=DEBUG, ems.appender
```

4 To specify that all received events from external EMS systems be logged:

➤ Locate the following lines in the file:

```
# Change ${emsloglevel} to DEBUG to see received events
log4j.category.EmsEventPrinter=${emsloglevel}, ems.appender
log4j.additivity.EmsEventPrinter=false
```

➤ Change the argument of the log4j.category.EmsEventPrinter parameter from ${emsloglevel} to DEBUG, as follows:

```
log4j.category.EmsEventPrinter=DEBUG, ems.appender
```

5 Save the file.

Troubleshooting Integration Monitors

The information below describes basic troubleshooting techniques that may be useful when working with Integration Monitors. Additional troubleshooting information is located in the Knowledge Base on the Mercury Customer Support web site (support.mercury.com).

➤ Look for errors in the <SiteScope root directory>\logs\EmsMonitors.log and <SiteScope root directory>\logs\error.log files.

➤ Increase the level of Integration Monitor logging in the EmsMonitors.log file to DEBUG. For details, see "Integration Monitor Logging Options" on page 1046.

➤ If samples are created and sent from SiteScope but cannot be seen in Mercury Business Availability Center Dashboard, Event Log, or SiteScope reports, look in the <Mercury Business Availability Center root directory>\log\core\dispatcher_log.txt file to make sure the samples were not dropped due to missing fields or values.

➤ Use the <Mercury Business Availability Center root directory>\bin\sprinter.exe utility to view the sample flow on the Bus. Run the executable without parameters to view usage instructions.

➤ Increase the level of Dashboard logging in the <Mercury Business Availability Center root directory\conf\core\Tools\log4j\EJB\ble.properties file to verify that Dashboard is receiving samples. Locate the following parameter and change the log level status to DEBUG:

log4j.category.Trinity.BLE_SAMPLES=DEBUG, trinity.samples.appender

In addition, look at the <Mercury Business Availability Center root directory\log\EJBContainer\TrinitySamples.log file.

102

Integration Monitor Configuration Files

You customize Integration Monitor configuration file templates to enable capturing event and metrics data from Enterprise Management Systems, automated support systems, and other management applications.

This chapter describes:	On page:
Introducing Integration Monitor Configuration Files	1049
Understanding Configuration File Structure	1051
Event Handler Structure	1052
Working with Configuration Files	1059

Introducing Integration Monitor Configuration Files

All Integration Monitors depend on configuration files, which define the processing of incoming data and define the output sample forwarded to Business Availability Center.

Integration Monitors designed for use with specific EMS applications can be configured in Monitor Administration without editing their configuration files. Their configuration files are predefined by Mercury and only require modification if specific customizations are required.

For Technology Integration Monitors (Technology SNMP Trap, Technology Log File, and Technology Database monitors), you must create an appropriate configuration file using one of the generic configuration file templates supplied before you configure the monitor in Monitor Administration. The Technology Web Service Integration Monitor configuration file may also need to be customized.

The locations of the predefined configuration files and the generic configuration file templates are listed below:

Integration Monitors for Specific EMS Applications

These configuration files are stored in the following locations:

<SiteScope root directory>/conf/ems/<monitor_type>/<name>.config

where **<SiteScope root directory>** is the SiteScope installation path, **<monitor_type>** is the monitor type name (for example, **tivoli**, **netiq**, or **hp**), and **<name>** is the name of an existing configuration file.

Technology Integration Monitors

These configuration files are stored in the following locations:

- Technology SNMP Trap, Technology Log File, and Technology Database Integration Monitors:

  <SiteScope root directory>/conf/ems/templates/<name>.config

  where **<SiteScope root directory>** is the SiteScope installation path and **<name>** is the name of a configuration file template.

- Technology Web Service Integration Monitor:

  <SiteScope root directory>/conf/ems/webservice/<name>.config

  where **<SiteScope root directory>** is the SiteScope installation path and **<name>** is the name of a configuration file template.

Understanding Configuration File Structure

The configuration files contain instructions on how to process the data as it arrives to the Integration Monitors. The configuration file is based on concept of event handlers—independent sections that contain instructions relevant to specific data. You can use these to customize the configuration to data that originated in several different Enterprise Management Systems.

The instructions that constitute the configuration file are grouped into event handlers. Each Integration Monitor has a configuration file containing one or more sets of event handlers. Each event handler contains a "matching condition," by which SiteScope can decide whether to use a particular event handler for an arriving event. When an event or data arrives at the Integration Monitor, it iterates over the different event handlers in the configuration file, in the order they appear in the file, testing the "matching condition" of each handler. If a matching handler is found, the monitor uses the instructions within that handler to process the event and perform the action defined for this handler (for example, forward it to Business Availability Center or discard). No further sections are checked after the first match. If no matches are found, the event is discarded. By default, each file comes with an event handler that matches all events.

In addition to the event handlers, the configuration file can contain special entries that affect the Integration Monitor engine as a whole. These values are grouped into the `[$DEFAULT_PARAMETERS$]` section. This section defines default values for tags that are common for all handlers. Any tag can be set in this section; it will be used to create a reported value unless overridden in the matched event handler. For each incoming event, this event handler will always be executed prior to the matched event handler.

For details on event handler structure, see “Event Handler Structure” on page 1052.

Tip: Always have a copy of the default or original configuration file available when you edit a configuration file, so that you will be able to consult the original settings if necessary.

Event Handler Structure

Each event handler has following structure:

```
[name]
Matching condition
Action directive
Tags
```

The names of **Matching condition**, **Action directive** and additional directives start with dollar sign symbol (**$**). The names of tags should not start with dollar sign.

Comments are allowed in the configuration file. The comment starts with either **#**, **!** or **;** character and continues to the end of the line.

This section includes the following topics:

- "Matching Condition" on page 1052
- "Basic String Expressions" on page 1056
- "Basic Conditional Expression" on page 1056
- "Action Directive" on page 1056
- "Tags" on page 1057
- "Integration Monitor Configuration File Examples" on page 1058

Matching Condition

The Match Condition must be a valid boolean expression. The expression can contain calls to the operators and functions defined below. The expression can access the contents of the event that is being processed using the dollar sign ($) notation. For example, if the incoming event is SNMP Trap, then its enterprise OID can be accessed as `$oid`. Refer to the user guide of the relevant monitor type for names specific to that monitor.

The matching condition has the form:

$MATCH=Boolean expression

where the Boolean expression is one of the expressions listed in the table below. When mentioned in the description, the expression can also be used to assign values into tags (see “Tags” on page 1057).

Boolean expression(s)	Description	Examples	True if.
<, <=, > , >=, ==, !=	Checks the numerical correctness of the expression. Can be used with `INT` or `DOUBLE` fields.	$MATCH= $numberOfLines == 100	field $numberOfLines equals 100
		$MATCH= $numberOfColumns <= 107	field $numberOfColumns equals 107 or less
equals(String)	Checks for string equality.	$MATCH= “ERROR”.equals($status)	field $status equals the word ERROR
		$MATCH= $status.equals(“ERROR”)	field $status equals the word ERROR
true, false	Constant Boolean values.	$MATCH= true	always true
&&, ||	To be used in order to combine any of the above boolean expressions.	$MATCH= $status.equals(“ERROR”) || $numberOfLines == 100	field $status equals the word ERROR or if field $numberOfLines equals 100

time()	Returns the current time in seconds since January 1, 1970 format. Can be used with `DOUBLE` fields.	$MATCH= $timeStampField > (time()-600)	the value of the $timeStampField is newer then ten minutes ago (in seconds since January 1, 1970 format)
parseInt(String), parseDouble(String),	Use to convert strings to numeric values. The input string should be a valid representation of an Integer or a floating point number. **Note:** calling this function on a string that cannot be interpreted as a number will cause an error and the incoming event will be dropped. Can also be used with `INT` or `DOUBLE` fields.	$MATCH= parseInt($size) > 10	the string value in the $size field is an integer bigger then 10

str_to_seconds(Str1,Str2)	Calculates the timestamp (in seconds since `January 1, 1970` format) held in the first String using the format in the second string. Can also be used with `DOUBLE` fields.	`$MATCH=` str_to_seconds ($time,"yyyy-MM-dd HH:mm:ss.SSS") > time() **Note:** use the following symbols to represent time data: Year - 'y' Month - 'M" Day of month - 'd' Hour - 'H' Minute - 'm' Second - 's'	the date specified in the `$time` field in the `"`yyyy-MM-dd HH:mm:ss.SSS `"` format is later than the current time. You can search for SimpleDateFormat on the Internet for more information
exist($field)	Checks for an existence of a field in the processed event and makes sure that it is not an empty value.	$MATCH= exist($status)	Field `$status` exists in the incoming event and is not an empty string
isInt(String), isDouble(String)	Checks if the input string can be interpreted as an integer or a double number, respectively.	$MATCH=isDouble($size)	The string value in the $size field can be converted to a double

Any of the above expressions can be used and the expression can refer to incoming event fields. The value of the expression, which can be either **true** or **false**, determines whether the event handler will be used to process the event or not.

Basic String Expressions

The following table summarizes the string expressions that can be used in the configuration files:

Operation	Description	Examples
+	String concatenation	“trap type is “ + $trap

Basic Conditional Expression

One conditional expression is supported; the **?** operator. This operator can be used to compose three expressions into one: **<Conditional part> ? <if true part> : <if false part>**

Action Directive

The action directive has form:

$ACTION= TOPAZ_BUS_POST or DISCARD

The value of the Action directive defines whether the event will be processed and forwarded to Business Availability Center, or discarded. This value will take effect only if the matching condition within the handler had been evaluated to positive value (that is, to **true**). The table below describes the effect of the different actions.

Action	Description	For use with
TOPAZ_BUS_POST (event)	Send the event to the Business Availability Center bus and database.	Mercury Business Availability Center
TOPAZ_BUS_POST (ss_t)	Send the metrics to Application Management as SiteScope Data.	Mercury Business Availability Center
DISCARD	Do not send the data to Mercury Business Availability Center	Events you wish to filter out.

Note: If you are using the metrics template, TOPAZ_BUS_POST(ss_t), the data is sent to the Mercury Business Availability Center database as SiteScope data, and thus saved to the database. For details on the metrics template, see "Configuring the Metrics Template (metrics.config)" on page 1065.

Tags

In addition to directives, event handler contains **tags**. Each tag represents a field in the event that will be forwarded to Business Availability Center, whose value can be evaluated when the event arrives to the Integration Monitor.

General form of a tag is:

name[:type]=value

The name is any string without spaces or dollar signs (**$**). The type specifies the type of field as reported to Business Availability Center. It can be either **INT**, **DOUBLE** or **STRING**. The default type is **STRING**.

By defining a tag, you can customize event forwarding to Business Availability Center and to get more value from the external applications that generate events that will be forwarded to the Business Availability Center Dashboard. If, for example, the monitor pulls out data from a database table column called `AlertText`, which contains a textual description of an alert, it is possible to send that data to Business Availability Center by adding the following line to an event handler section:

```
[event handler]
$MATCH=true
$ACTION=TOPAZ_BUS_POST(event)
text=$AlertText
```

Note: When adding tags, always add them after the **$MATCH** and **$ACTION**.

Integration Monitor Configuration File Examples

Example 1: Universal Event Handler

```
[post them all]
$MATCH=true
$ACTION=TOPAZ_BUS_POST(event)
severity:INT=SEVERITY_INFORMATIONAL
szAlarmText:STRING=”post them all handler received an event”
```

Note that the **$MATCH** directive in the handler is set to **true**. This causes every event to match the handler and therefore every event is sent to the Business Availability Center Bus.

Example 2: Different Event Handlers for Different Severities

```
[Error Handler]
$MATCH= $status.equals(“ERROR”)
$ACTION=TOPAZ_BUS_POST(event)
severity:INT=SEVERITY_CRITICAL

[Info Handler]
$MATCH= $status.equals(“INFO”)
$ACTION=TOPAZ_BUS_POST(event)
severity:INT=SEVERITY_INFORMATIONAL

[post them all]
$MATCH=true
$ACTION=TOPAZ_BUS_POST(event)
severity:INT=SEVERITY_INFORMATIONAL
```

In the example above, an incoming event will be matched against the **Error Handler** event handler. If the handlers condition is true (that is, the value in the status field equals **ERROR**), then an event with a field called severity, whose value is **SEVERITY_CRITICAL**, will be sent to Mercury Business Availability Center. An event can only be matched by a single handler: The first match will stop the processing and therefore once an event is matched by a section it will not be processed by the next handler.

If the event was not matched by the first handler, the second handler will come into action and its match (which looks for status of **INFO**) will be used to decide whether the second handler needs to take action. Finally, If the event does not match the second handler, the third, universal handler will be evaluated.

Working with Configuration Files

This section describes how to customize predefined configuration files or Technology Integration Monitor configuration file templates.

Note:

- Use only the mandatory and optional fields defined in the templates when working with the default configuration file templates. See the tables in the following sections for more information.
- You should make a backup copy of the template configuration files and use a copy of the template files for any modifications that your make. This will allow you to restore the default configuration if necessary.
- You must customize the generic Technology Integration Monitor configuration file template before you configure a Technology Integration Monitor in Monitor Administration. All mandatory fields must be set in the template to ensure that the applicable monitor is configured correctly.

This section includes the following topics:

- Configuring the Event Template (event.config)
- Configuring the Metrics Template (metrics.config)

Configuring the Event Template (event.config)

The event template is used for extracting events collected by external system and importing them to Business Availability Center.

This section includes the following topics:

- Mandatory Values for the Event Template
- Optional Values for the Event Template
- Conditional Expression Example 1:
- Conditional Expression Example 2:
- Event File Example

Mandatory Values for the Event Template

The tables below list mandatory and optional values for the event template.

Field Name	Type	Description	Example
time_stamp	DOUBLE	Time stamp in seconds since Jan 1 1970	time_stamp:DOUBLE=str_to_seconds($time,"yyyy-MM-dd HH:mm:ss.SSS").
severity	INT	One of the following severities: SEVERITY_UNKNOWN SEVERITY_INFORMATIONAL SEVERITY_WARNING SEVERITY_MINOR SEVERITY_MAJOR SEVERITY_CRITICAL	severity:INT=SEVERITY_MINOR
target_name	STRING	Name of device or host that generated the event	target_name=$hostName
status	STRING	Status of event in external EMS terminology	status=”OPEN”

subject	STRING	Subject of event (e.g. CPU , SAP application, Hard Disk), middle/high level hierarchy describing the event source. The hierarchy describing an event is in the following format: monitor_group (optional) --> target_name --> object (optional) --> subject --> instance. More levels can be added above monitor monitor_group by using logical_group, and attr1 - 5.	subject=”DISK”
instance	STRING	Instance of subject that generated the event (e.g D:\ ). Lowest level of hierarchy describing the event source	instance=”E:\\”
description	STRING	Textual description of event	description="free space on drive e is below 10%"
data_source	STRING	System that generated the event	data_source=”HP OVO”

Optional Values for the Event Template

The tables below list optional values for the event template.

Field Name	Type	Description	Example
target_ip	STRING	IP of host or device that generated the event	target_ip=$IPString
object	STRING	Optional level in the hierarchy describing the event source	object="OS"
event_id	STRING	Unique identifier of this event	event_id=$id
logical_group	STRING	Logical grouping of this event	logical_group=”error messages”
monitor_group	STRING	Monitor group that reported this event	monitor_group="log monitors on \\hostname"
orig_severity_name	STRING	Severity in external EMS terminology	orig_severity_name ="Cleared"
acknowledged_by	STRING	Name of user that acknowledged this event	acknowledged_by =$username
owner	STRING	Name of user who owns this event	owner="admin"

value	DOUBLE	Use to transfer numerical values from the event	value=$thresholdViolated
attr1	STRING	Extra data slot	attr1=$history
attr2	STRING	Extra data slot	attr2=$moreHistory
attr3	STRING	Extra data slot	attr3="Design"
attr4	STRING	Extra data slot	attr4=$MonitorOutput
attr5	STRING	Extra data slot for long strings	attr5=$Longhistory

Conditional Expression Example 1:

```
severity:INT=$var6.equals(“red”) ? SEVERITY_CRITICAL
: SEVERITY_INFORMATIONAL
```

In this example, the value of sixth variable binding is compared to string red. If the variable binding is indeed equal to string red, then the value of the severity tag will be set to SEVERITY_CRITICAL, otherwise it will be set to SEVERITY_INFORMATIONAL.

Conditional Expression Example 2:

```
severity:INT=$var6.equals(“red”) ? SEVERITY_CRITICAL :
$var6.equals(“green”) ? SEVERITY_INFORMATIONAL : $var6.equals(“yellow”)
? SEVERITY_MINOR : SEVERITY_WARNING
```

This example chains the conditional operator into a decision chain. If the sixth variable binding holds string red, then severity tag will have the value SEVERITY_CRITICAL. If the sixth variable binding holds string green, then severity tag will have the value SEVERITY_INFORMATIONAL. If the variable binding holds string yellow, the tag will have the value SEVERITY_MINOR. If none of the above conditions are true, then the tag will have the value SEVERITY_WARNING.

Event File Example

In the example below , two types of events are sent: the first are events of status "OPEN" and the second are events cleared by a user. The data is retrieved from incoming event fields using the $ notation. All other events are discarded by the last handler.

```
[$DEFAULT_PARAMETERS$]
#####################################################
# NOTE: the following parameters are mandatory #
#####################################################
time_stamp:DOUBLE=str_to_seconds($time,"yyyy-MM-dd HH:mm:ss.SSS")
severity:INT= SEVERITY_UNKNOWN
target_name=$Device
status=$Status
subject="EMS X Events"
instance=$target
description=$description
data_source="EMS X"

#send an open event with the value in value fields and with the event id
[OPEN events]
$MATCH="OPEN".equals($Status)
$ACTION=TOPAZ_BUS_POST(event)
value:DOUBLE=parseDouble($threshold)
event_id=$uid

#send clear events with the event id and acknowledging username
[clear events]
$MATCH="CLEAR".equals($Status)
$ACTION=TOPAZ_BUS_POST(event)
event_id=$uid
acknowledged_by=$ClearedBy

[event sink]
$MATCH=true
$ACTION=DISCARD
```

Configuring the Metrics Template (metrics.config)

The metrics template is used for extracting metrics collected by external system and importing them to Business Availability Center. The metrics will be reported to Business Availability Center as SiteScope metrics. The metrics template defines a mandatory structure.

This section includes the following topics:

- Mandatory Values for the Metrics Template
- Metrics Template Example

Mandatory Values for the Metrics Template

The table below lists mandatory values for the metrics template.

Field Name	Type	Description	Example
TimeStamp	DOUBLE	Time stamp in the seconds since Jan 1st 1970 format	TimeStamp:DOUBLE=time()
Quality	INT	Quality in SiteScope terms. Possible values are: `QUALITY_ERROR`, `QUALITY_WARNING`, `QUALITY_GOOD`	Quality:INT= QUALITY_ERROR
MonitorName	STRING	Logical monitor name	MonitorName=”NT cpu Monitor”
MonitorState	STRING	The monitor status, for example, N\A, Good, Error, and so forth.	MonitorState=”Received ” + $count + “ events”

MonitorType	STRING	The monitor type	MonitorType=”System Monitor”
TargetName	STRING	The target of this monitor (e.g. host name)	TargetName=$Device
MeasurementName(N)	STRING	Name *Nth* measurement	MeasurementName(1)=”CPU Temperature”
Value(N)	DOUBLE	Value of Nth measurement	Value(1):DOUBLE=$CPUTemperature

Metrics Template Example

In the example below, two metrics are sent: the first one (MeasurementName (1)) takes its name from the `$legend` field and takes the value from the `$value` field. A second metric (Measurement Name (2)) uses the constant name `CPU Temperature` which receives its value from the `$CPUTemp` field.

```
##########################################
#            EMS Integration metricsconfig file  #
# use this file to send metrics to Mercury Business Availability Center #
##########################################
[$DEFAULT_PARAMETERS$]
# time stamp in the seconds since Jan 1st 1970 format.
TimeStamp:DOUBLE=str_to_seconds($time,"yyyy-MM-dd HH:mm:ss.SSS")

# quailty in SiteScope terms QUALITY_ERROR, QUALITY_WARNING,
QUALITY_GOOD
Quality:INT=QUALITY_ERROR

# Logical monitor name
MonitorName=$kpName

#target, e.g. host name
TargetName=$parentMachineName

#the status string of the monitor (e.g.: “Log file read, 3 matches found”)
MonitorState=”The monitor status is: “+ $status
```

```
#the monitor type (e.g. “Log Monitor”, “CPU Monitor”)
MonitorType=”NetIQ measurements”

#measurement name
MeasurementName(1)=$legend
#value as double
Value(1):DOUBLE=parseDouble($value)

#measurement name
MeasurementName(2)=”CPU Temperature”
#value as double
Value(2):DOUBLE=parseDouble($CPUTemp)
#########################################################
# To send more than one measurement per DB row #
# add pairs #
# MeasurementName (* ) = #
# Value (*) :DOUBLE= #
# where * = 1,2,.,n #
# #######################################################
[allR]
$MATCH=true
$ACTION=TOPAZ_BUS_POST(ss_t)
```

When specifying more than one metric in the template, a separate sample will be sent with each of the metrics.

Note: When specifying multiple metrics per file, the metric numbering must be consecutive.

In the case of failure, errors will appear in the **EmsMonitors.log** but the error will not affect the monitor status.

103

Avalon Event Monitor

The Avalon Lancelot suite provides real-time statistical and trend data allowing IT staff to monitor and manage IP traffic and to maintain the efficiency and health of infrastructure, system and applications. It can generate events when one of the aspects crosses a threshold (defined in the Avalon Lancelot console). The Avalon Event Monitor allows you to integrate these events into the Mercury Business Availability Center system, eliminating the need to check manually for the events.

This chapter describes:	On page:
About the Avalon Event Monitor	1069
Setup Requirements	1070
Configuring the Avalon Event Monitor	1071

About the Avalon Event Monitor

The Avalon Event Monitor is useful for forwarding events generated by the Lancelot network monitoring suite to Mercury Business Availability Center. The Lancelot suite provides real-time statistical and trend data allowing IT staff to monitor and manage IP traffic and to maintain the efficiency and health of infrastructure, system and applications.

Each time an event is generated by the Avalon Lancelot network management suite, it can be forwarded to Mercury Business Availability Center using the Avalon Event Monitor. While receiving and forwarding events, SiteScope can log the events for you, eliminating the need to check for the events generated by the Avalon Lancelot manually. In addition, you can be notified of warning conditions that you might have otherwise been unaware of until something more serious happened. Each time that it runs this monitor, SiteScope checks events that have been received since the last time the monitor ran.

The Avalon Event monitor uses a pre-defined configuration file to define the processing of incoming data and define the output sample forwarded to Mercury Business Availability Center. If you have to make any specific customizations, you can modify this configuration file. For details, see "Integration Monitor Configuration Files" on page 1049.

Note: For information on Integration Monitor logging and troubleshooting, see "Integration Monitor Logging Options" and "Troubleshooting Integration Monitors" in Chapter 101, "Working with SiteScope Integration Monitors."

Note: If you are upgrading SiteScope from version 7.8.1.2 or 7.9.0.0, see the note about upgrading Integration Monitor types for version 7.9.1.0 or later in the section "Working with SiteScope Integration Monitors"

Setup Requirements

The following are requirements for using the Avalon Event Monitor to forward events to Mercury Business Availability Center:

- The Avalon server needs to be configured to send traps to the SiteScope server.

Note: The Avalon Event Monitor receives events from Avalon Lancelot suite as SNMP Traps. For that purpose it must have sole access to UDP port 162 (this is SNMP Trap UDP port). If another application (including another instance of SiteScope, running, for example, as a process) uses this port, the Avalon Event Monitor will report an "Address in use" error while defining the monitor. However, the Avalon Event Monitor can share this port with other SiteScope monitors that must receive SNMP traps.

- SiteScope must be registered with a Mercury Business Availability Center installation. The SiteScope must have a profile defined in the Mercury Business Availability Center installation prior to enabling the registration in the SiteScope interface. In order to verify registration or to re-register SiteScope with the Mercury Business Availability Center server, see the Mercury Business Availability Center Server Registration page under SiteScope Preferences.

Configuring the Avalon Event Monitor

The Avalon Event Monitor should be added to a SiteScope monitor group created for this monitor and other Integration Monitor types. It is recommended that you configure Integrations Monitors only after a connection between the SiteScope and Mercury Business Availability Center is established.

Note: SiteScope cannot be deployed behind a firewall. The SiteScope and the monitored system must be on the same LAN or special firewall configuration may be required.

Main Settings for the Avalon Event Monitor

You use the Main Settings section to specify the text name used for this monitor instance in the interface. Complete the entry in the Main Settings section as described below, and click the **OK** button to save the settings.

Name

Enter a text name for this Avalon Event monitor instance. This text is displayed in the Monitor Administration interface and in the SiteScope interface. If you do not enter a name text, a default name will be used.

Advanced Settings for the Avalon Event Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Avalon Event Monitor and its display in the product interface. Use this section to set monitor-to-monitor dependencies, customize display options, and configure other settings specific to the Avalon Event Monitor that may be required in some infrastructure environments. Complete the entries as needed and click the **OK** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

EMS Configuration File Path

Enter the path to the EMS integration configuration file relative to the SiteScope installation. The default location is: <SiteScope root directory>\conf\ems\Avalon\event.config.
For more information about the format of the file see the section “Integration Monitor Configuration Files” on page 1049.

If you want to edit this file, create a copy on the SiteScope machine and work in the new copy. Then, in Monitor Administration, edit the path to the new file.

Frequency

Select how often the monitor should update its status. The **Frequency** setting for the Avalon Event Monitor controls only the status reports. The Avalon events are forwarded when they are received without any delay. The default interval is to update once every 10 minutes. Use the drop-down list to the right of the text box to specify an update interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Run Alerts

Choose the method for running alerts. If "for each event received from Avalon system " is chosen, then the monitor triggers alerts for every matching entry found.

Note: When the Avalon Event Monitor is run in the "for each event received from Avalon system" alert method, the monitor will never report a status of error or warning, regardless of the results of the content match or even if the target SNMP Trap is not found.

If the "once, after all events from Avalon system were received" method is chosen, then the monitor counts up the number of matches and triggers alerts based on the "Error If" and "Warning If" thresholds defined for the monitor in the Threshold Settings section.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. You may, however, schedule your monitors to run only on certain days or on a fixed schedule. Click the Edit schedule link to create or edit a monitor schedule. For more information about working with monitor schedules, see the section on Schedule Preferences for Monitoring.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the other monitor should have for the current monitor to run normally. The current monitor will be run normally as long as the monitor selected in the **Depends On** field reports the condition selected in this field. For example, by selecting OK, this monitor is only enabled as long as the monitor selected in the **Depends On** field reports a status of good or OK.

Monitor Description

Enter additional information to describe this monitor. The Monitor Description can include HTML tags such as the <BR>, <HR>, and <B> tags to control display format and style. The description text will appear on the Monitor Detail page.

Report Description

Enter an optional description for this monitor that will make it easier to understand what the monitor does. For example, network traffic or main server response time. This description will be displayed on with each bar chart and graph in Management Reports and appended to the tool-tip displayed when you pass the mouse cursor over the status icon for this monitor on the Monitor Detail page.

EMS Time Difference

Use this option to account for time differences between the system clock time on the monitored EMS machine and the server where SiteScope is running. This is only needed when the EMS data includes time data and the time data shows that there is a time difference between the EMS machine and the SiteScope server. If the time difference is too great the data may be discarded from Mercury Business Availability Center.

Note: The time difference value only needs to be entered if the difference is greater than one minute. There is no need to synchronize differences of seconds less than one minute.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. When an error is detected, the monitor will immediately be scheduled to run again once.

Note: In order to change the run frequency of this monitor when an error is detected, you should use the **Error Frequency** option instead of the **Verify Error** option.

Note: The status returned by the **Verify Error** run of the monitor will replace the status of the originally scheduled run that detected an error. This may cause the loss of important performance data if the data from the verify run is different than the initial error status.

Use of this option across many monitor instances may result in significant monitoring delays in the case that multiple monitors are rescheduled to verify errors at the same time.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the status of this Avalon Event monitor instance based on the results returned by the check.

Each Avalon Event monitor instance has three status settings:

- **Error if**
- **Warning if**
- **Good if**

You can set unlimited threshold criteria for each status condition per Avalon Event monitor instance. By default, only one threshold is displayed when you first configure the monitor.

While the monitor is enabled, it is assigned a status of good, warning, or error based on the most recent execution of the monitor action. The measurement taken or the results reported by the monitor are tested against the status threshold settings to determine the status.

The individual results are combined as logical **OR** relationships when more than one threshold condition is defined for any of the three settings. When one or more of the conditions (for example when two conditions for **Error if** setting) are met for a status setting the monitor status is set to the corresponding status condition. If status conditions are met for more than one status setting the status of the monitor is set to the highest valued status condition. For example, if one condition selected as Error if and another condition selected as Warning if are both met, the status would be reported as an error, with **error** being the highest value, **warning** the next highest and **good** the lowest value. The status is displayed by color and a status icon in the SiteScope interface.

A change of status signals an event and acts as a trigger for alerts associated with the monitor or the group to which the monitor belongs.

A change of status may also effect the state of a dependency between monitors. For example, a monitor that detects a change that results in a error status may be a trigger to disable one or more other monitors that are dependent on the Avalon events.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement value. You may use the default status thresholds defined for the Avalon Event or use the following steps to change the monitor status thresholds for this monitor instance:

To edit monitor status thresholds:

1. Use the first drop down menu to for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop down menu to select the comparison operator(s) that will define the status threshold.

3 Enter a value applicable to the measurement parameter in the third text box.

4 To add another threshold setting, click the **New Error If** button and repeat the steps above.

5 Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

104

BMC PATROL Event Monitor

The BMC PATROL Event Monitor allows you to integrate existing BMC PATROL installations and transfer Open Events from your BMC PATROL Agents to your Mercury Business Availability Center installation. This monitor supports BMC PATROL Agent versions 3.4, 3.5, and 3.6 installed on any operating system.

This chapter describes:	On page:
About the BMC PATROL Event Monitor	1079
Integration Architecture	1082
KM Installation and Configuration	1084
Connectivity Settings	1087
Connectivity Diagnostics	1088
Configuring the BMC PATROL Event Monitor	1089

About the BMC PATROL Event Monitor

The BMC PATROL Event Monitor requires a custom PATROL knowledge module to be installed on one central agent and a second PATROL knowledge module to be installed on all PATROL Agents whose events you want to integrate with Mercury Business Availability Center.

Once the BMC Patrol Event Monitor/KM combination is installed and configured, every new BMC PATROL event is transferred to the Mercury Business Availability Center installation.

In addition to transferring the BMC PATROL events to Mercury Business Availability Center, the BMC Patrol Event Monitor is capable of discovering the configuration of BMC PATROL Agents on a subnet. The configuration is then available to the Mercury Business Availability Center Dashboard.

Operating Environments

This monitor must be used in conjunction with two KMs installed on BMC PATROL Agents. The KMs are responsible for delivering **Open** events to the BMC Patrol Event Monitor. The BMC Patrol Event Monitor collates events as reported from BMC PATROL Agents into unified samples and delivers these samples to the Mercury Business Availability Center server.

The BMC PATROL Event monitor uses a pre-defined configuration file to define the processing of incoming data and define the output sample forwarded to Mercury Business Availability Center. If you have to make any specific customizations, you can modify this configuration file. For details, see "Integration Monitor Configuration Files" on page 1049.

The Patrol Agent/Console must be installed on the SiteScope machine. This enables the use of the Patrol Agent Open API which is needed for discovering the BMC configuration process. Discovering the BMC configuration process requires access to the files **pemapi.dll** and **acmmls32.dll**. These files are available as part of either the BMC Patrol Agent or the BMC Patrol Console, and are usually located in the **<%PATROL_HOME>/bin** folder. To ensure that the monitor can access the files, you must specify the path to the files, unless the location of the files is already specified in the %PATH% (search path).

Note: If you are working with BMC secure environment, you have to set your environment to enable use of PATROL components (use of pemapi component for example). Otherwise, configuration retrieval is not possible.

Limitations

BMC integration works only with SiteScope installed in a Windows environment. There is no BMC integration support for SiteScope installed in a UNIX environment.

If you work with Mercury Business Availability Center version 5.1 and lower, you cannot define new BMC monitors or edit existing ones within Mercury Business Availability Center's Monitor Administration. This is because of variances in the user interface. You define new monitors or edit existing ones using the SiteScope interface. First detach the SiteScope from Monitor Administration, define or edit the monitor, and then reattach the SiteScope to Monitor Administration. For details attaching and detaching a SiteScope, see "Removing a SiteScope from Monitor Administration" in *Managing SiteScope*.

The BMC monitor should be defined or edited only in SiteScope's new user interface.

About Scheduling This Monitor

Since the reading and status collected by the BMC Patrol Event Monitor include only statistical information, the monitor does not have to be scheduled very often. Scheduling the BMC Patrol Event Monitor to run every 10 minutes should be sufficient.

Reading and Status

The monitor reading shows the number of events received since the last scheduled update or manual refresh, together with the number of currently connected agents.

Note: The event counter goes down to zero each time the monitor is refreshed. This is expected behavior.

Note: For information on Integration Monitor logging and troubleshooting, see "Integration Monitor Logging Options" on page 1046 and "Troubleshooting Integration Monitors" on page 1047.

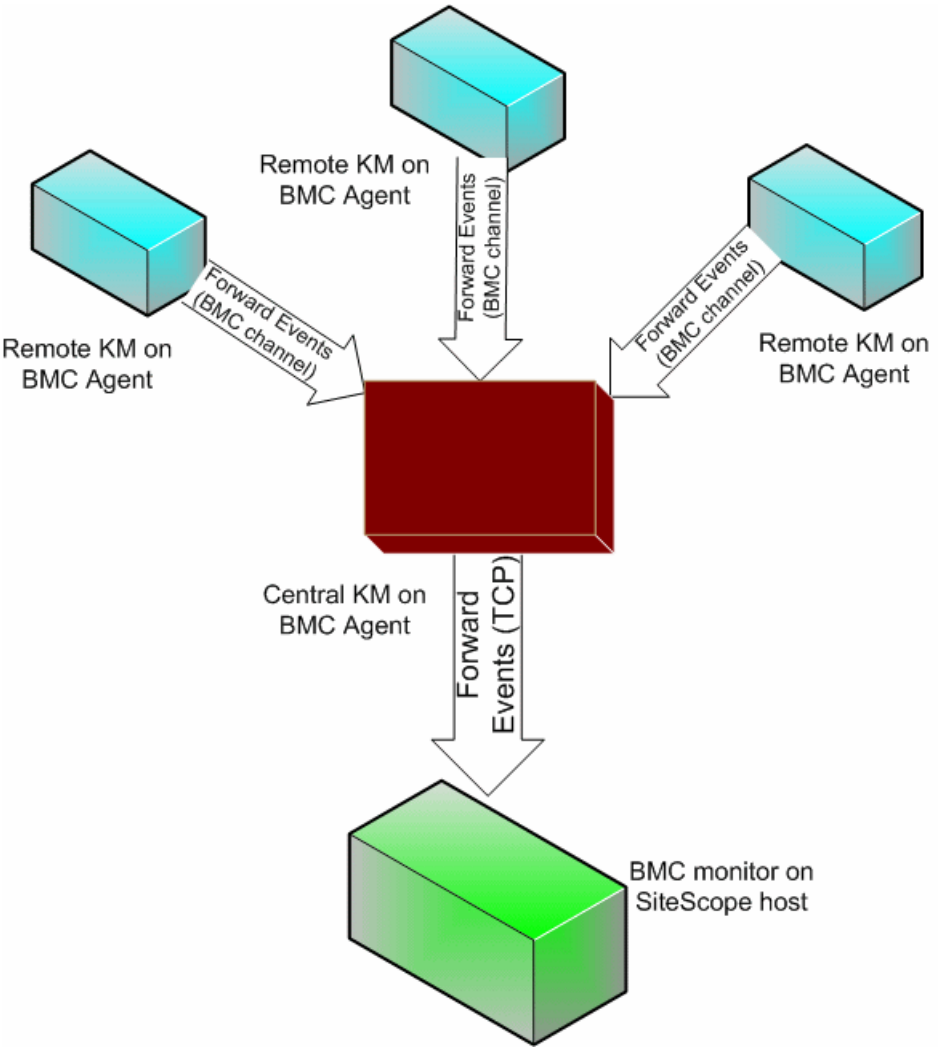
Integration Architecture

The integration consists of one central agent that receives events from all agents whose events you want passed to Mercury Business Availability Center. The connection between the remote agents and the central agent uses BMC communication (BMC secure channel). The connection between the central agent and SiteScope uses a TCP socket to the SiteScope BMC monitor.

The KM that is installed on the remote agent queries all events of defined types and forwards them to the central agent using PSL commands. The KM that is installed on the central machine queries all events of type remote event and forwards them to the bmc_mercury process. This process forwards the events to the monitor using a TCP socket.

If the central agent is installed on the SiteScope host, the integration is fully secured. It is recommended not to install a SiteScope running many monitors with many configurations on the same machine as the central agent. It is preferable to choose a SiteScope with fewer monitors and configurations for this purpose. If you choose to install SiteScope on a separate machine and you work with a secure environment, you must install

SiteScope with one of the secured BMC agent's machine to enable the configuration retrieval. The integration forwards all open, acknowledged, or closed events of BMC class 9, 11, and 39. Events that have a status of acknowledged or closed may be forwarded with a five minute delay. This is because the process for checking these statuses (acknowledge and close) runs only every five minutes to avoid high CPU utilization.



KM Installation and Configuration

The KM must be installed and configured on the BMC agent machines in order to have the events forwarded to SiteScope and then to Mercury Business Availability Center. The following are the procedures you follow to install and configure the KM package.

Installing the Mercury_Central_Agent.km on the Central Agent

The integration uses BMC sending channels which are secured. By installing the BMC central agent on the SiteScope machine itself, the integration is fully secured. You can install the central agent on a machine that is not the SiteScope machine, but the channel between the central agent and the SiteScope machine is then not as secure. If you do install **Mercury_Central_Agent.km** on a machine other than the SiteScope machine, that machine must be running in a Windows environment.

To install the Mercury_Central_Agent.km on the Central Agent:

1. Navigate to **<SiteScope root directory>\conf\ems\bmc\addon\central**.
2. From that location, copy **mercury_central_agent** library to **<BMC root directory>\Patrol3**.
3. From the same location copy **Mercury_Central_Agent.km** and **Mercury_Remote_Messages.ctg** to **<BMC root directory>\Patrol3\lib\knowledge** directory.
4. Open the PATROL Developer Console.
5. Use **File** > **Load KM menu** to load the **Mercury_Central_Agent.km** file (change the **Files of Type** selection to **KM files** to display the Mercury_Central_Agent.km file).
6. Select the **Desktop** tab. Under the **Central Agent host**, right click the **Mercury_Central_Agent.km** file and choose **KM Commands** > **CreateCentralAgentConnectionParams**.

   This creates the file **central_agent_params.ini** in the **<BMC root directory>\Patrol3\mercury_central_agent** directory. This file contains the details of the central agent to be used by all remote agents. This file is necessary for the deployment of all remote agents.

7 Copy the generated file to **<SiteScope root directory>\conf\ems\bmc\addon\remote\mercury_remote_agent** directory.

Configuring the Central Agent

Use the following procedure to configure the central agent.

To configure the Central Agent machine:

1 Select the **Desktop** tab. Right-click each host and select **Development** > **Agent Configuration**.

Warning: Use care when working with the **Console** in developer mode. Changes that you make may destroy data or configuration settings.

---

2 On the configuration window, browse to **MERCURY/BAC**.

3 In the right section, double click **SiteScope_Address**.

4 Double click **REPLACE = "127.0.0.1"** (or any other value that is set).

5 Change the value to the IP address of the SiteScope machine that you will use to configure the BMC Patrol Event Monitor. Click **OK**.

6 Double click **REPLACE = "1789"** (or any other value that is set).

7 Change the value to the port that is used for monitoring this group of Patrol agents with the BMC Patrol Event Monitor. Click OK.

8 Click **OK**.

9 Choose **Tools** > **Apply Configuration**.

10 Select the central host to which you want to apply the configuration changes. Click **OK**.

11 Close the configuration window (there is no need to save).

Installing the Mercury_Remote_Messages.km on Remote Agents

Follow this procedure for each remote agent.

To install the Mercury_Remote_Messages.km on remote agents:

1. Deploy the directory <**SiteScope root directory**>**\conf\ems\bmc\addon\remote\mercury_remote_agent** (containing the generated file) to all remote agents under <**BMC root directory**>**\Patrol3**.
2. Deploy from <**SiteScope root directory**>**\conf\ems\bmc\addon\remote** the files **Mercury_Remote_Messages.km** and **Mercury_Remote_Messages.ctg** to the <**BMC root directory**>**\Patrol3\lib\knowledge** directory in all remote agents.
3. For all remote agents, load the **Mercury_Remote_Messages.km**.

General Agent Configuration

Each agent saves its events in case these events cannot be forwarded. The default time limit is fifteen minutes. The time limit is to prevent the flooding of events to SiteScope during a long period that there is no communication from the agent. The time period to save the events can be modified with the following procedure.

To modify the time period to save events on the agent:

1. Open the **PATROL Developer Console**.
2. Select **Development** > **Agent Configuration**.
3. In the left screen, select the **MERCURY/BAC** directory.
4. In the right screen, double click on the variable **RangeSaveEvents**.
5. In the small box, double click **Replace**.
6. In the dialog box that opens, enter the number of minutes to save the events.
7. Click **OK** to save and close.
8. Select **Tools** > **Apply Configuration**.
9. Choose the applicable server and click **OK**.
10. Close the window (there is no need to save).

Configure the KM for Preload

You should configure the KM modules to be preloaded by the agent after you have completed the installation. This will configure the KM to be loaded whenever the agent is restarted. It also eliminates the need for the console to be open for the KM to be loaded and accessible.

To configure the KM for preload:

1. Open the PATROL Developer Console.
2. Select **Development** > **Agent Configuration**.
3. In the left screen, select the agent setup directory.
4. In the right screen, double click the variable **preLoadedKm**.
5. In the small box, double click **Replace**.
6. In the dialog box that opens, enter the name of the km (**Mercury_Central_Agent.km** or **Mercury_Remote_Messages.km**).
7. Click **OK** to save and close.
8. Select **Tools** > **Apply Configuration**.
9. Choose the applicable server and click **OK**.
10. Close the window (there is no need to save).

Connectivity Settings

There are four ways in which the monitor can be configured to connect to the BMC agent. You can change this configuration by editing the Patrol monitor configuration file found at <SiteScope root directory>\conf\ems\bmc\bmc_comm.cfg.

Every change in that file requires restarting the SiteScope server.

The options are:

- Use a UDP protocol when attempting to connect to the BMC agent and ping the agent before trying to connect to it (PROTOCOL=UDP, PING=1).

Using this option, the monitor will ping the agent before trying to connect to it and only if the agent is accessible, will it connect to it using UDP protocol.

➤ Use UDP protocol when attempting to connect to the BMC agent and do not ping the agent before trying to connect to it (PROTOCOL=UDP, PING=0).

Using this option, the monitor will connect to the agent using UDP protocol without checking if it is accessible.

➤ Use TCP protocol when attempting to connect to the BMC agent and do not ping the agent before trying to connect to it (PROTOCOL=TCP, PING=0).

Keep in mind that when using this option, there is TCP access to the agent. The BMC API function which is used to connect the agent is a blocking function. This means that the function will wait until it acquires a connection to the agent. This can last around four minutes (depending on the OS) and may cause socket exceptions and bad monitoring functionality.

Use this option only if you are sure that you have TCP access to all the agents.

➤ Use TCP protocol when attempting to connect the BMC agent and ping the agent before trying to connect to it (PROTOCOL=TCP, PING=1).

This is the default behavior. The monitor will check if the agent is accessible by trying to ping it. Only if the agent is accessible, will the monitor try to connect the agent through TCP protocol.

Using this option ensures that the BMC API function does not wait for the connection and does not cause undesirable results.

Connectivity Diagnostics

You use the following steps to verify connectivity with the PATROL agents.

To verify connectivity to the PATROL Agent(s):

1 After installing the PATROL monitor, open a command prompt window, and change the working directory to the <SiteScope root directory>\bin directory.

2 Run the PATROL connection diagnostic utility, bmc_mercury_tools, using the following command line syntax:

bmc_mercury_tools <server name> <user name> <port number>

where the command line arguments are defined as follows:

<server name> - targeted BMC PATROL Agent computer name

<user name> - PATROL user name with permissions to contact the above PATROL Agent

<port number> - PATROL Agent connection port (usually 3181)

You will be prompted for a corresponding password.

3 If the connection is successful, the following file will be created in the location indicated: <SiteScope root directory>/bin/BmcMercuryToolsXmlData.xml.

4 The BmcMercuryToolsXmlData.xml describes the metrics sampled by the PATROL Agent in XML format. In addition to the log files, five results of CPU Processor Time Percent are displayed on the console.

Note: If the remote PATROL Agent is running on UNIX, the CPU Processor Time Percent metrics will be reported as errors. These errors do not necessarily indicate failure to connect to the PATROL Agent. This is because the test is trying to sample nt_cpu which does not exist on UNIX machines.

---

5 If the connection fails, an error message is reported. Additional information is available in the file <SiteScope root directory>\logs\bmc_mercury_comm.txt.

Configuring the BMC PATROL Event Monitor

The BMC PATROL Event Monitor should be added to a SiteScope monitor group created for this monitor and other Integration Monitor types. It is recommended that you configure Integrations Monitors only after a connection between the SiteScope and Mercury Business Availability Center is established.

Note: SiteScope cannot be deployed behind a firewall. The SiteScope and the monitored system must be on the same LAN or special firewall configuration may be required.

Main Settings for the BMC PATROL Event Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the Patrol Agent counter data and the text name used for this monitor instance in the interface. Complete the entries in the Main Settings section as described below. Complete the entries as needed and click the **OK** button to save the settings.

Name

Enter a text name for this BMC PATROL Event monitor instance. This text is displayed in the Monitor Administration interface and in the SiteScope interface. If you do not enter a name text, a default name will be used.

Advanced Settings for the BMC PATROL Event Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the BMC PATROL Event Monitor and its display in the product interface. Use this section to set monitor-to-monitor dependencies, customize display options, and configure other settings specific to the BMC PATROL Event Monitor that may be required in some infrastructure environments. Complete the entries as needed and click the **OK** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

EMS Configuration File Path

Enter the path to the EMS integration configuration file relative to the SiteScope installation. The default location is: <SiteScope root directory>\conf\ems\bmc\event.config. For more information about the format of the file see the section "Integration Monitor Configuration Files" on page 1049.

If you want to edit this file, create a copy on the SiteScope machine and work in the new copy. Then, in Monitor Administration, edit the path to the new file.

Frequency

Select how often the monitor should update its status. The **Frequency** setting for the BMC PATROL Event Monitor controls only the status reports. The Patrol Agent counter data are forwarded when they are received without any delay. The default interval is to update once every 10 minutes. Use the drop-down list to the right of the text box to specify an update interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

PATROL Mercury BAC Integration TCP Port

Enter the TCP port number as configured in the PTI Application. By default, default TCP port number 1789 is used. If you need to use a different port number, see the section "KM Installation and Configuration" on page 1084 for instructions on how to configure the port number.

Old Add-on Installed

Select only if your BMC system has PTI installed. PTI is the add-on that was used in previous versions to connect between BMC and SiteScope. If you are upgrading from SiteScope 7.9.5.0 and you already have defined monitors that work with the old PTI, they are automatically marked as working with old add-on installed.

UDP Communication Protocol

Select this option if you want to use UDP as the communication protocol when getting topology data from the BMC agents. The default communication protocol is TCP.

There are four options to use in configuring the monitor to connect to the BMC agent to retrieve configuration data. For details, see "Connectivity Settings" on page 1087.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. You may, however, schedule your monitors to run only on certain days or on a fixed schedule. Click the Edit schedule link to create or edit a monitor schedule. For more information about working with monitor schedules, see the section on Schedule Preferences for Monitoring.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the other monitor should have for the current monitor to run normally. The current monitor will be run normally as long as the monitor selected in the **Depends On** field reports the condition selected in this field. For example, by selecting OK, this monitor is only enabled as long as the monitor selected in the **Depends On** field reports a status of good or OK.

Monitor Description

Enter additional information to describe this monitor. The Monitor Description can include HTML tags such as the <BR>, <HR>, and <B> tags to control display format and style. The description text will appear on the Monitor Detail page.

Report Description

Enter an optional description for this monitor that will make it easier to understand what the monitor does. For example, network traffic or main server response time. This description will be displayed on with each bar chart and graph in Management Reports and appended to the tool-tip displayed when you pass the mouse cursor over the status icon for this monitor on the Monitor Detail page.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely

- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the status settings to set threshold conditions that determine the status of this BMC PATROL Event monitor instance based on the results returned by the check.

Each BMC PATROL Event monitor instance has three status settings:

- **Error if**
- **Warning if**
- **Good if**

While the monitor is enabled, it is assigned a status of good, warning, or error based on the most recent execution of the monitor action. The measurement taken or the results reported by the monitor are tested against the status threshold settings to determine the status. The status is displayed by color and a status icon in the SiteScope interface.

A change of status acts as a trigger for alerts associated with the monitor or the group to which the monitor belongs. For example, if the BMC PATROL Event Monitor detects that the Patrol Agent counter data has become unavailable, the status change from good to error is used to trigger an alert on error.

A change of status may also effect the state of a dependency between monitors.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement value. You may use the default status thresholds defined for the BMC PATROL Event or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop down menu to for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. Repeat these steps for the Warning if and Good if settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Settings for Configuration Retrieval

Define the agents to which you want to connect in the configuration retrieval process. Use this area to define the details of each of the agents for which you want to see configuration data. You can add as many agents as you need. For each agent, enter the host/ip to use for the connection. If you enter a host, it is converted to an ip so the ip is displayed in the Mercury Business Availability Center Dashboard. All the agents defined must be reachable in the network.

For each agent, you must define the user name/password/port to use for the connection.

Note: If you are upgrading from SiteScope 7.9.5.0 and you have monitors which were defined in version 7.9.5.0 and working with the old PTI, the configuration data of the agents that were defined in the configuration retrieval settings and the agents that are connected to the old monitors will be combined.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

105

BMC PATROL Metrics Monitor

The BMC PATROL Metrics Monitor allows you to collect metrics collected by Patrol Agents and forward them to Mercury Business Availability Center.

This chapter describes:	On page:
About the BMC PATROL Metrics Monitor	1097
System Requirements	1098
Connectivity Diagnostics	1098
Configuring the BMC PATROL Metrics Monitor	1100

About the BMC PATROL Metrics Monitor

Use the BMC PATROL Metrics Monitor to collect all the metrics monitored by Patrol Agents both on NT and UNIX machines. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate monitor instance for each Patrol Agent in your environment.

The BMC Patrol Metrics Monitor connects to the Patrol Agent using Patrol-provided libraries (Patrol Agent API). You will also need to know the Patrol's user name, user password, port number used to connect to the Patrol Agent.

Note: For information on Integration Monitor logging and troubleshooting, see Integration Monitor Logging Options and Troubleshooting Integration Monitors in Chapter 101, "Working with SiteScope Integration Monitors."

System Requirements

Patrol Agent/Console must be installed on the SiteScope machine (enables the use of the Patrol Agent Open API).

The BMC Patrol Metrics Monitor requires access to the files pemapi.dll and acmmls32.dll. These files are available as part of either the BMC Patrol Agent or the BMC Patrol Console, and are usually located in the <%PATROL_HOME>\bin folder. To ensure that the monitor can access the files, you specify the path to the files, unless the location of the files are already specified in the %PATH% (search path).

Connectivity Diagnostics

You can use the **bmc_mercury_tools** application to check that communication is available to a BMC Patrol Agent and that the BMC Patrol Metrics Monitor installation was performed correctly.

Note: Collecting metrics from remote PATROL Agents involves PATROL-to-PATROL communication, which is known to have reliability issues. If you are experiencing problems while integrating PATROL metrics, you should restart the PATROL Agent.

To verify connectivity to the Patrol Agent(s):

1 After installing the Patrol monitor, open a command prompt window, and change the working directory to the <SiteScope root directory>\bin directory.

2 Run the Patrol connection diagnostic, **bmc_mercury_tools**, with the following command line syntax:

bmc_mercury_tools <server name> <user name> <port number>

where the command line arguments are defined as follows:

<server name> - targeted BMC Patrol Agent computer name

<user name> - Patrol user name with permissions to contact the above Patrol Agent

<port number> - Patrol Agent connection port

You will be prompted for a corresponding password.

3 If the connection is successful, the following file will be created in the location indicated: <SiteScope root directory>/bin/BmcMercuryToolsXmlData.xml

The BmcMercuryToolsXmlData.xml file describes the metrics sampled by the PATROL Agent in XML format. In addition to the log files, five results of CPU Processor Time Percent are displayed on the console.

Note: If the remote PATROL Agent is running on UNIX OS, the CPU Processor Time Percent metrics will be reported as errors. These errors do not necessarily indicate failure to connect to the PATROL Agent. The reason is that the test is trying to sample nt_cpu which doesn't exist on UNIX machines.

---

4 If the connection fails, an error message is reported. Additional information regarding the connectivity to the agent is available in the file <SiteScope root directory>\logs\bmc_mercury_comm.txt.

Configuring the BMC PATROL Metrics Monitor

The BMC PATROL Metrics Monitor should be added to a SiteScope monitor group created for this monitor and other Integration Monitor types. It is recommended that you configure Integrations Monitors only after a connection between the SiteScope and Mercury Business Availability Center is established.

Note: SiteScope cannot be deployed behind a firewall. The SiteScope and the monitored system must be on the same LAN or special firewall configuration may be required.

Main Settings for the BMC PATROL Metrics Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the Patrol agents, how often this BMC PATROL Metrics Monitor instance should be run, and the text name used for this monitor instance in the interface. Complete the entries in the Main Settings section as described below. Complete the entries as needed and click the **OK** button to save the settings.

Name

Enter a text name for this BMC PATROL Metrics monitor instance. This text is displayed in the Monitor Administration interface and in the SiteScope interface. If you do not enter a name text, a default name will be used.

Frequency

Select how often the BMC PATROL Metrics monitor checks metrics from the Patrol agents to forward to Mercury Business Availability Center. The default interval is to update once every 10 minutes. Use the drop-down list to the right of the text box to specify an update interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Patrol Agent Address

Choose the server you want to monitor (the server must have a PATROL agent installed and running).

Patrol API Port

Set the configuration port for the BMC Patrol agent (default is 3181).

Patrol Username

Give patrol agent user name which will be used when communicating with the agent.

Patrol Password

Give patrol agent user password which will be used when communicating with the agent.

Counters

You select the counters to be monitored by the BMC PATROL Metrics Monitor using the expandable menu tree feature. The menu tree is automatically populated after you enter valid connection properties and then click the **Get Counters** button. Use the selection features in the counters menu tree to expand or contract the counter tree and select the counters you want to monitor with this monitor instance.

Advanced Settings for the BMC PATROL Metrics Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the BMC PATROL Metrics Monitor and its display in the product interface. Use this section to set monitor-to-monitor dependencies, customize display options, and configure other settings specific to the BMC PATROL Metrics Monitor that may be required in some infrastructure environments. Complete the entries as needed and click the **OK** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. You may, however, schedule your monitors to run only on certain days or on a fixed schedule. Click the Edit schedule link to create or edit a monitor schedule. For more information about working with monitor schedules, see the section on Schedule Preferences for Monitoring.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the other monitor should have for the current monitor to run normally. The current monitor will be run normally as long as the monitor selected in the **Depends On** field reports the condition selected in this field. For example, by selecting OK, this monitor is only enabled as long as the monitor selected in the **Depends On** field reports a status of good or OK.

Monitor Description

Enter additional information to describe this monitor. The Monitor Description can include HTML tags such as the <BR>, <HR>, and <B> tags to control display format and style. The description text will appear on the Monitor Detail page.

Report Description

Enter an optional description for this monitor that will make it easier to understand what the monitor does. For example, network traffic or main server response time. This description will be displayed on with each bar chart and graph in Management Reports and appended to the tool-tip displayed when you pass the mouse cursor over the status icon for this monitor on the Monitor Detail page.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. When an error is detected, the monitor will immediately be scheduled to run again once.

Note: In order to change the run frequency of this monitor when an error is detected, you should use the **Error Frequency** option instead of the **Verify Error** option.

Note: The status returned by the **Verify Error** run of the monitor will replace the status of the originally scheduled run that detected an error. This may cause the loss of important performance data if the data from the verify run is different than the initial error status.

Use of this option across many monitor instances may result in significant monitoring delays in the case that multiple monitors are rescheduled to verify errors at the same time.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the status of this BMC PATROL Metrics monitor instance based on the results returned by the check for measurements from.

Each BMC PATROL Metrics monitor instance has three status settings:

- **Error if**
- **Warning if**
- **Good if**

You can set unlimited threshold criteria for each status condition per BMC PATROL Metrics monitor instance. By default, only one threshold is displayed when you first configure the monitor.

While the monitor is enabled, it is assigned a status of good, warning, or error based on the most recent execution of the monitor action. The measurement taken or the results reported by the monitor are tested against the status threshold settings to determine the status.

The individual results are combined as logical **OR** relationships when more than one threshold condition is defined for any of the three settings. When one or more of the conditions (for example when two conditions for **Error if** setting) are met for a status setting the monitor status is set to the corresponding status condition. If status conditions are met for more than one status setting the status of the monitor is set to the highest valued status condition. For example, if one condition selected as Error if and another condition selected as Warning if are both met, the status would be reported as an error, with **error** being the highest value, **warning** the next highest and **good** the lowest value. The status is displayed by color and a status icon in the SiteScope interface.

A change of status signals an event and acts as a trigger for alerts associated with the monitor or the group to which the monitor belongs.

A change of status may also effect the state of a dependency between monitors. For example, a monitor that detects a change that results in a error status may be a trigger to disable one or more other monitors that are dependent on the Patrol agents.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement value. You may use the default status thresholds defined for the BMC PATROL Metrics or use the following steps to change the monitor status thresholds for this monitor instance:

To edit monitor status thresholds:

1. Use the first drop down menu to for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

106

CA Unicenter Event Monitor

The CA Unicenter Event Monitor allows you to integrate an existing CA Unicenter installation with Mercury Business Availability Centerby transferring CA Unicenter events to an Business Availability Center server. This monitor supports CA Unicenter Event Management versions 2.x or 3.x running on the Windows operating system.

This chapter describes:	On page:
About the CA Unicenter Event Monitor	1109
System Requirements	1110
Configuring the CA Unicenter Event Monitor	1115

About the CA Unicenter Event Monitor

The CA Unicenter Event Monitor makes use of Mercury-supplied integration module (called an add-on) that must be installed on the CA Unicenter Event Management server. Once the SiteScope CA Unicenter Event Monitor is configured and running, it collects events from CA Unicenter server as these are posted to the Unicenter log, and transfers the events to Mercury Business Availability Center via SiteScope.

The CA Unicenter Event monitor uses a pre-defined configuration file to define the processing of incoming data and define the output sample forwarded to Mercury Business Availability Center. If you have to make any specific customizations, you can modify this configuration file. For details, see “Integration Monitor Configuration Files” on page 1049.

Monitor Status

The status reading returned by the monitor is the current value of the monitor, such as `Received 10 events since the last update`. The status is logged as either OK, warning, or error. The status can be configured further using the Advanced Options in the CA Unicenter Event Monitor Configuration Form.

Note: For information on Integration Monitor logging and troubleshooting, see "Integration Monitor Logging Options" on page 1046 and "Troubleshooting Integration Monitors" on page 1047.

System Requirements

The following are important guidelines and requirements for using the CA Unicenter Event Monitor.

Note: If you are upgrading SiteScope from version 7.8.1.2 or 7.9.0.0, see the note about upgrading Integration Monitor types for version 7.9.1.0 or later in the section "Working with SiteScope Integration Monitors" on page 1043.

Operating Environment

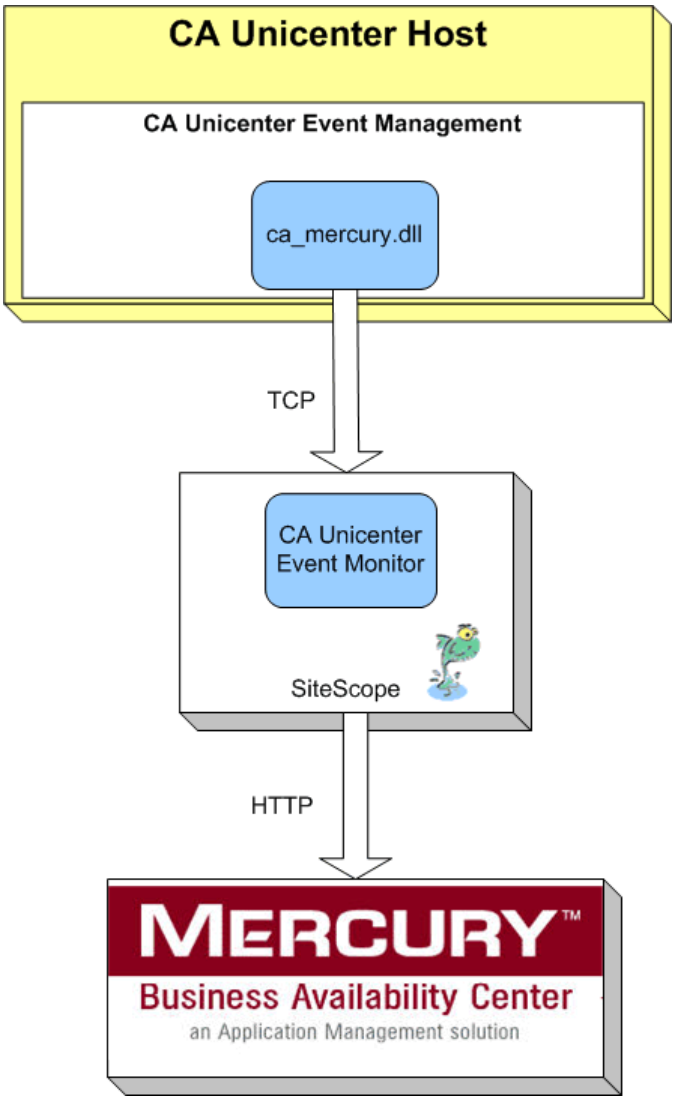
CA Unicenter Event Monitor supports CA Unicenter Event Management versions 2.x or 3.x running on the Windows operating system.

The CA Unicenter Event Monitor depends on a Mercury Interactive CA Integration Add-on module to collect events from the CA Unicenter server. The Add-on, when installed on the CA Unicenter Event Management server machine, listens to events received by the CA Unicenter system. The CA Unicenter Event Monitor, installed on a SiteScope machine, transfers the event data to Mercury Business Availability Center. The add-on and the monitor communicate using TCP/IP networking (using a customizable TCP port).

Note: The Mercury CA Unicenter Add-on is incompatible with CA Advanced Correlation Engine (ACE) or with any other software component that use CA Unicenter "user exits library" connection mechanism, since CA Unicenter allows only one library to be registered within the Event Management to receive its notifications.

About the CA Integration Add-on

The purpose of the CA Integration Add-on is to connect to the CA message infrastructure, to receive events from the CA and to forward these events to the SiteScope machine. The following diagram describes the functional relationship of the Mercury CA Integration Add-on, SiteScope, and the other applicable systems.



Installing the CA Integration Add-on

The following is an outline of the steps you use for the CA Integration Installation Process:

1. Install and configure the CA Integration Add-on on the CA Unicenter Event Management server.
2. Activate the CA Integration Add-on.
3. Activate the CA Unicenter Event Monitor.

The following section describes the steps for preparing, installing, activating, and configuring the Integration Add-on.

Before Installing the CA Integration Add-on

Prior to installation of the CA Integration Add-on, make sure you know the IP address (or network name) of the SiteScope machine on which the monitor is installed.

Installing the CA Integration Add-on

Use the following steps to install the CA Integration Add-on module.

To install the CA Integration Add-on module:

1. Copy the CA Integration Add-on module installation executable to the server where CA Unicenter Event Management is installed. The Add-on setup file path is <SiteScope root directory>\conf\ems\ca\addon\MercuryCAAddonSetup.exe.
2. Run the installation executable. The installation setup verifies if the machine contains a CA Unicenter installation. If no CA Unicenter is present, a warning message is displayed.
3. The setup verifies that no other "user exits library" presents in the CA Unicenter Event Management (Unicenter is restricted to only one entry). If another integration is present, a warning message is displayed.
4. Enter the SiteScope information as indicated (machine name, port, version). The setup process tries to verify the SiteScope information. If fails, a warning message is displayed. If the setup successfully verifies the SiteScope connection, the setup process continues.
5. The setup process asks if you want to restart the Unicenter.

Note: You must restart the Unicenter application in order to activate the add-on module.

Starting and Stopping the CA Integration Add-on

The CA Integration Add-on is connected to the CA Unicenter Event Management through the "user exits library" mechanism provided by CA. The library (a Windows DLL) receives Unicenter events as they enter the Unicenter console and forwards them to the SiteScope.

The CA Integration Add-on starts running once you restart the CA Unicenter after the add-on installation.

The CA Integration Add-on Configuration File

The CA Integration Add-on configuration is stored in the ca_mercury.cfg file in the /dat directory under the add-on installation root. The file is not expected to be edited by the user when default add-on configuration is used. The file contains several settings related to the SiteScope that the add-on is connected to: machine name, version and other (those settings are filled automatically by the add-on setup). Also, it contains the following definitions under the CAMercury section:

- SendOnlyHeldMessages (true/false) - indicates whether the add-on should forward to the SiteScope all CA Unicenter console messages or only "held messages". The default value is: false.
- HeldMessagesType (SENDKEEP) - indicates the type of held messages to be forwarded to the SiteScope. Currently, "SENDKEEP" is the only supported type.
- HeldMessagesAckText - since two messages are posted to the Unicenter console when a held message is acknowledged, this text indicates which of the two should be posted to the SiteScope as the acknowledgement message. The default value is: "CAOP_I_REPLYISSUED".
- UseLongMachineNames (true/false) - indicates whether the Unicenter message node machine names should be resolved by the add-on to fully qualified DNS names (for example "server.company.com") or to short

names (for example "server"). Changing of this setting may affect the behavior of several Mercury Business Availability Center applications with respect to the CA Unicenter Event monitor data handling (for example the dashboard view will show the long names together with the short ones that appeared before the change). The default value is: false.

There are also other settings that are used for internal purposes.

CAMercuryLog section contains settings related to the add-on log: log file directory, log level and other.

The CA Integration Add-on Log File

The CA Integration Add-on logs its activity to the log files. The log files are created when the add-on is started. Their names and locations are defined in the `ca_mercury.cfg` file in the `dat` directory under the add-on installation root directory.

Configuring the CA Unicenter Event Monitor

The CA Unicenter Event Monitor should be added to a SiteScope monitor group created for this monitor and other Integration Monitor types. It is recommended that you configure Integrations Monitors only after a connection between the SiteScope and Mercury Business Availability Center is established.

Note: SiteScope cannot be deployed behind a firewall. The SiteScope and the monitored system must be on the same LAN or special firewall configuration may be required.

Main Settings for the CA Unicenter Event Monitor

You use the Main Settings section to specify the text name used for this monitor instance in the interface. Complete the entry in the Main Settings section as described below, and click the **OK** button to save the settings.

Name

Enter a text name for this CA Unicenter Event monitor instance. This text is displayed in the Monitor Administration interface and in the SiteScope interface. If you do not enter a name text, a default name will be used.

Advanced Settings for the CA Unicenter Event Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the CA Unicenter Event Monitor and its display in the product interface. Use this section to set monitor-to-monitor dependencies, customize display options, and configure other settings specific to the CA Unicenter Event Monitor that may be required in some infrastructure environments. Complete the entries as needed and click the **OK** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

EMS Configuration File Path

Enter the path to the EMS integration configuration file relative to the SiteScope installation. The default location is: <SiteScope root directory>\conf\ems\ca\event.config. For more information about the format of the file see the section “Integration Monitor Configuration Files” on page 1049.

If you want to edit this file, create a copy on the SiteScope machine and work in the new copy. Then, in Monitor Administration, edit the path to the file.

Frequency

Select how often the monitor should update its status. The **Frequency** setting for the CA Unicenter Event Monitor controls only the status reports. The CA Unicenter event data are forwarded when they are received without any delay. The default interval is to update once every 10 minutes. Use the drop-down list to the right of the text box to specify an update interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

CA Unicenter Add-on TCP Port

Enter the TCP port number as configured in the CA Integration Add-on. By default port 9875 is used.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. You may, however, schedule your monitors to run only on certain days or on a fixed schedule. Click the Edit schedule link to create or edit a monitor schedule. For more information about working with monitor schedules, see the section on Schedule Preferences for Monitoring.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the other monitor should have for the current monitor to run normally. The current monitor will be run normally as long as the monitor selected in the **Depends On** field reports the condition selected in this field. For example, by selecting OK, this monitor is only enabled as long as the monitor selected in the **Depends On** field reports a status of good or OK.

Monitor Description

Enter additional information to describe this monitor. The Monitor Description can include HTML tags such as the <BR>, <HR>, and <B> tags to control display format and style. The description text will appear on the Monitor Detail page.

Report Description

Enter an optional description for this monitor that will make it easier to understand what the monitor does. For example, network traffic or main server response time. This description will be displayed on with each bar chart and graph in Management Reports and appended to the tool-tip displayed when you pass the mouse cursor over the status icon for this monitor on the Monitor Detail page.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. When an error is detected, the monitor will immediately be scheduled to run again once.

Note: In order to change the run frequency of this monitor when an error is detected, you should use the **Error Frequency** option instead of the **Verify Error** option.

Note: The status returned by the **Verify Error** run of the monitor will replace the status of the originally scheduled run that detected an error. This may cause the loss of important performance data if the data from the verify run is different than the initial error status.

Use of this option across many monitor instances may result in significant monitoring delays in the case that multiple monitors are rescheduled to verify errors at the same time.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the status of this CA Unicenter Event monitor instance based on the results returned by the check.

Each CA Unicenter Event monitor instance has three status settings:

- **Error if**
- **Warning if**
- **Good if**

You can set unlimited threshold criteria for each status condition per CA Unicenter Event monitor instance. By default, only one threshold is displayed when you first configure the monitor.

While the monitor is enabled, it is assigned a status of good, warning, or error based on the most recent execution of the monitor action. The measurement taken or the results reported by the monitor are tested against the status threshold settings to determine the status.

The individual results are combined as logical **OR** relationships when more than one threshold condition is defined for any of the three settings. When one or more of the conditions (for example when two conditions for **Error if** setting) are met for a status setting the monitor status is set to the corresponding status condition. If status conditions are met for more than one status setting the status of the monitor is set to the highest valued status condition. For example, if one condition selected as Error if and another condition selected as Warning if are both met, the status would be reported as an error, with **error** being the highest value, **warning** the next highest and **good** the lowest value. The status is displayed by color and a status icon in the SiteScope interface.

A change of status signals an event and acts as a trigger for alerts associated with the monitor or the group to which the monitor belongs.

A change of status may also effect the state of a dependency between monitors. For example, a monitor that detects a change that results in a error status may be a trigger to disable one or more other monitors that are dependent on the CA Unicenter event data.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement value. You may use the default status thresholds defined for the CA Unicenter Event or use the following steps to change the monitor status thresholds for this monitor instance:

To edit monitor status thresholds:

1. Use the first drop down menu to for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

107

Compaq Insight Manager Event Monitor

The Compaq Insight Manager Event Monitor watches for reports on health and availability of monitored devices arriving from Compaq Insight Manager. It alerts you on any events received by the Compaq Insight Manager system and reports data to Mercury Business Availability Center. This monitor enables you to monitor Compact Insight Manager version 7.0 installed on any operating system.

This chapter describes:	On page:
About the Compaq Insight Manager Event Monitor	1123
Setup Requirements	1124
Configuring the Compaq Insight Manager Event Monitor	1125

About the Compaq Insight Manager Event Monitor

The Compaq Insight Manager Event Monitor watches for reports on health and availability of monitored devices arriving from Compaq Insight Manager. It alerts you of any event reported by the Compaq Insight Manager system.

Note: For information on integration monitor logging and troubleshooting, see "Integration Monitor Logging Options" on page 1046 and "Troubleshooting Integration Monitors" on page 1047.

Note: If you are upgrading SiteScope from version 7.8.1.2 or 7.9.0.0, see the note about upgrading Integration Monitor types for version 7.9.1.0 or later in the section "Working with SiteScope Integration Monitors" on page 1043.

Setup Requirements

The following are requirements for using the Compaq Insight Manager Event Monitor:

- You must use one of the database drivers supplied by default, or install or copy a compatible database driver or database access API into the appropriate SiteScope directory location. The supplied drivers include:

  com.inet.tds.TdsDriver - (TDS driver from i-net Software for Microsoft SQL databases)

  com.inet.ora.OraDriver - (JDBC thin driver for Oracle databases)

  Many other database driver packages are available as compressed (zipped) archive files or .jar files. Database drivers in this form must NOT be extracted and must be installed into the <SiteScope root directory>\java\lib\ext subdirectory.

- You need to know the syntax for the Database Connection URL. The Database Connection URL normally includes the class of driver you are using, some key name relating to the supplier of the driver software, followed by a combination of server, host, and port identifiers. Examples of database connection URL's are:

  `jdbc:inetdae:`*`hostname`*`:`*`port`* - (where *`hostname`* is the name of the host where the database is running and *`port`* is the port on which the database interfaces with the driver)

  `jdbc:oracle:thin:@`*`hostname`*`:`*`port`*`:`*`dbname`* - (where *`hostname`* is the name of the host where the database is running, *`port`* is the port on which the database interfaces with the driver, and *`dbname`* is the name of the Oracle database instance)

- The database you want to query must be running, have a database name defined, and have at least one named table created in the database. In some cases, the database management software needs to be configured to allow connections via the middleware or database driver.
- You need a valid username and password to access and perform a query on the database. In some cases, the machine and user account that SiteScope is running on must be given permissions to access the database.

  The Compaq Insight Manager Event monitor uses a pre-defined configuration file to define the processing of incoming data and define the output sample forwarded to Mercury Business Availability Center. If you have to make any specific customizations, you can modify this configuration file. For details, see "Integration Monitor Configuration Files" on page 1049.

Configuring the Compaq Insight Manager Event Monitor

The Compaq Insight Manager Event Monitor should be added to a SiteScope monitor group created for this monitor and other Integration Monitor types. It is recommended that you configure Integrations Monitors only after a connection between the SiteScope and Mercury Business Availability Center is established.

Note: SiteScope cannot be deployed behind a firewall. The SiteScope and the monitored system must be on the same LAN or special firewall configuration may be required.

Main Settings for the Compaq Insight Manager Event Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the Compaq Insight Manager, how often this Compaq Insight Manager Event Monitor instance should be run, and the text name used for this monitor instance in the interface. Complete the entries in the Main Settings section as described below. Complete the entries as needed and click the **OK** button to save the settings.

Name

Enter a text name for this Compaq Insight Manager Event monitor instance. This text is displayed in the Monitor Administration interface and in the SiteScope interface. If you do not enter a name text, a default name will be used.

Frequency

Select how often the monitor should update its status. The **Frequency** setting for the Compaq Insight Manager Event Monitor controls only the status reports. The Compaq Insight Manager are forwarded when they are received without any delay. The default interval is to update once every 10 minutes. Use the drop-down list to the right of the text box to specify an update interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Database Connection URL

Enter a URL to a Database Connection (sometimes referred to as an Authentication string). One way to create a database connection is to use ODBC to create a named connection to a database. For example, first use the ODBC control panel to create a Data Source Name (DSN) called test under the system DSN tab. Then, enter jdbc:odbc:test in this box as the connection URL. Other way is to use the supplied MS SQL or Oracle driver in order to connect to the Database. When using the MS SQL driver, use the connection URL of the form jdbc:inetdae:<computer_name>:<port>?database=<db_name>. When using the Oracle driver, use the connection URL of the form jdbc:inetora:<computer_name>:<port>:<instance>.

Database Driver

Enter the driver used to connect to the database. Use the Fully Qualified Class Name of the JDBC driver you wish to use. The default drivers for this monitor are the com.inet.tds.TdsDriver - (TDS driver from i-net Software for Microsoft SQL databases) or oracle.jdbc.driver.OracleDriver - (JDBC thin driver for Oracle 7 and 8 databases). When using OBBC-JDBC connection, you may use sun.jdbc.odbc.JdbcOdbcDriver.

Database Username

Enter the username used to login to the database.

Database Password

Enter a password used to login to the database.

Advanced Settings for the Compaq Insight Manager Event Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Compaq Insight Manager Event Monitor and its display in the product interface. Use this section to set monitor-to-monitor dependencies, customize display options, and configure other settings specific to the Compaq Insight Manager Event Monitor that may be required in some infrastructure environments. Complete the entries as needed and click the **OK** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

EMS configuration file path

Enter the path to the EMS integration configuration file relative to the SiteScope installation. The default location is: <SiteScope root directory>\conf\ems\cim\event.config. For more information about the format of the file see the section "Integration Monitor Configuration Files" on page 1049.

If you want to edit this file, create a copy on the SiteScope machine and work in the new copy. Then, in Monitor Administration, edit the path to the file.

Maximum Number of Rows to Retrieve

Specify the maximum number of rows the monitor retrieves from the database for each monitor cycle. The default value is 5000.

If the number of result rows exceeds the set maximum, the monitor will retrieve the remaining rows (those that exceeded the maximum) on future cycles, until all result rows are retrieved.

The Max Rows value should be large enough to keep up with database table growth, yet small enough to avoid java.lang.OutOfMemoryException errors. Further, monitor run frequency should also be considered. Make sure that the rate at which data is collected by the monitor—which is dependent upon both monitor run frequency and network/system speed—is greater than or equal to the rate of data insertion on the monitored system.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. You may, however, schedule your monitors to run only on certain days or on a fixed schedule. Click the Edit schedule link to create or edit a monitor schedule. For more information about working with monitor schedules, see the section on Schedule Preferences for Monitoring.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the other monitor should have for the current monitor to run normally. The current monitor will be run normally as long as the monitor selected in the **Depends On** field reports the condition selected in this field. For example, by selecting OK, this monitor is only enabled as long as the monitor selected in the **Depends On** field reports a status of good or OK.

Monitor Description

Enter additional information to describe this monitor. The Monitor Description can include HTML tags such as the <BR>, <HR>, and <B> tags to control display format and style. The description text will appear on the Monitor Detail page.

Report Description

Enter an optional description for this monitor that will make it easier to understand what the monitor does. For example, network traffic or main server response time. This description will be displayed on with each bar chart and graph in Management Reports and appended to the tool-tip displayed when you pass the mouse cursor over the status icon for this monitor on the Monitor Detail page.

EMS Time Difference

Use this option to account for time differences between the system clock time on the monitored EMS machine and the server where SiteScope is running. This is only needed when the EMS data includes time data and the time data shows that there is a time difference between the EMS machine and the SiteScope server. If the time difference is too great the data may be discarded from Mercury Business Availability Center.

Note: The time difference value only needs to be entered if the difference is greater than one minute. There is no need to synchronize differences of seconds less than one minute.

DB Machine Name

If you are reporting monitor data to an installation of Mercury Business Availability Center, enter a text identifier describing the database server that this monitor is monitoring. This text descriptor is used to identify the database server when the monitor data is viewed in a Mercury Business Availability Center report. Use only alphanumeric characters for this entry. You can enter the name of the monitored server or a description of the database that will be used to identify the host.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. When an error is detected, the monitor will immediately be scheduled to run again once.

Note: In order to change the run frequency of this monitor when an error is detected, you should use the **Error Frequency** option instead of the **Verify Error** option.

Note: The status returned by the **Verify Error** run of the monitor will replace the status of the originally scheduled run that detected an error. This may cause the loss of important performance data if the data from the verify run is different than the initial error status.

Use of this option across many monitor instances may result in significant monitoring delays in the case that multiple monitors are rescheduled to verify errors at the same time.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the status settings to set threshold conditions that determine the status of this Compaq Insight Manager Event monitor instance based on the results returned by the check for event data from.

Each Compaq Insight Manager Event monitor instance has three status settings:

- **Error if**
- **Warning if**
- **Good if**

While the monitor is enabled, it is assigned a status of good, warning, or error based on the most recent execution of the monitor action. The measurement taken or the results reported by the monitor are tested against the status threshold settings to determine the status. The status is displayed by color and a status icon in the SiteScope interface.

A change of status acts as a trigger for alerts associated with the monitor or the group to which the monitor belongs. For example, if the Compaq Insight Manager Event Monitor detects that the Compaq Insight Manager has become unavailable, the status change from good to error is used to trigger an alert on error.

A change of status may also effect the state of a dependency between monitors.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement value. You may use the default status thresholds defined for the Compaq Insight Manager Event or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop down menu to for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. Repeat these steps for the Warning if and Good if settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

108

Concord Metrics Monitor

You use the Concord Metrics Monitor to collect data from a Concord database and forward them to Mercury Business Availability Center. This monitor enables you to monitor Concord version 5.6 installed on any operating system.

This chapter describes:	On page:
About the Concord Metrics Monitor	1135
Setup Requirements	1136
Configuring the Concord Metrics Monitor	1137

About the Concord Metrics Monitor

Each time the Concord Metrics Monitor runs, it transfers new metrics from the Concord database to the Mercury Business Availability Center as time series data.

The Concord Metrics monitor uses a pre-defined configuration file to define the processing of incoming data and define the output sample forwarded to Mercury Business Availability Center. If you have to make any specific customizations, you can modify this configuration file. For details, see "Integration Monitor Configuration Files" on page 1049.

Note: For information on Integration Monitor logging and troubleshooting, see "Integration Monitor Logging Options" on page 1046 and "Troubleshooting Integration Monitors" on page 1047.

Setup Requirements

The following are key system requirements for using the Concord Metrics Monitor:

Note: If you are upgrading SiteScope from version 7.8.1.2 or 7.9.0.0, see the note about upgrading Integration Monitor types for version 7.9.1.0 or later in the section "Working with SiteScope Integration Monitors" on page 1043.

- You must use one of the database drivers supplied by default, or install or copy a compatible database driver or database access API into the appropriate SiteScope directory location. The supplied drivers include:

  com.inet.tds.TdsDriver - (TDS driver from i-net Software for Microsoft SQL databases)

  com.inet.ora.OraDriver - (JDBC thin driver for Oracle databases)

  Many other database driver packages are available as compressed (zipped) archive files or .jar files. Database drivers in this form must NOT be extracted and must be installed into the <SiteScope root directory>/java/lib/ext subdirectory.

- You need to know the syntax for the Database Connection URL. The Database Connection URL normally includes the class of driver you are using, some key name relating to the supplier of the driver software, followed by a combination of server, host, and port identifiers. Examples of database connection URLs are:

  jdbc:inetora:<*hostname*>:<*port*>:<*dbname*> - (where hostname is the name of the host where the database is running, port is the port on which the

database interfaces with the driver, and dbname is the name of the Oracle database instance)

jdbc:oracle:thin:@*hostname:port:dbname* - (where *hostname* is the name of the host where the database is running, *port* is the port on which the database interfaces with the driver, and *dbname* is the name of the Oracle database instance)

- The Oracle server that contains the Concord repository you want to query must be running.
- You need a valid username and password to access and perform a query on the database.

Configuring the Concord Metrics Monitor

The Concord Metrics Monitor should be added to a SiteScope monitor group created for this monitor and other Integration Monitor types. It is recommended that you configure Integrations Monitors only after a connection between the SiteScope and Mercury Business Availability Center is established.

Note: SiteScope cannot be deployed behind a firewall. The SiteScope and the monitored system must be on the same LAN or special firewall configuration may be required.

Main Settings for the Concord Metrics Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the Concord database for metrics, how often this Concord Metrics Monitor instance should be run, and the text name used for this monitor instance in the interface. Complete the entries in the Main Settings section as described below. Complete the entries as needed and click the **OK** button to save the settings.

Name

Enter a text name for this Concord Metrics monitor instance. This text is displayed in the Monitor Administration interface and in the SiteScope interface. If you do not enter a name text, a default name will be used.

Frequency

Select how often the Concord Metrics monitor checks the database for metrics to forward to Mercury Business Availability Center. The default interval is to update once every 10 minutes. Use the drop-down list to the right of the text box to specify an update interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Database Connection URL

Enter a URL to a Database Connection (sometimes referred to as an Authentication string). One way to create a database connection is to use ODBC to create a named connection to a database. For example, first use the ODBC control panel to create a Data Source Name (DSN) called test under the system DSN tab. Then, enter jdbc:odbc:test in this box as the connection URL. Other way is to use the supplied MS SQL or Oracle driver in order to connect to the Database. When using the MS SQL driver, use the connection URL of the form jdbc:inetdae:<computer_name>:<port>?database=<db_name>. When using the Oracle driver, use the connection URL of the form jdbc:inetora:<computer_name>:<port>:<instance>.

Database Driver

Enter the driver used to connect to the database. Use the Fully Qualified Class Name of the JDBC driver you wish to use. The default drivers for this monitor are the com.inet.tds.TdsDriver - (TDS driver from i-net Software for Microsoft SQL databases) or oracle.jdbc.driver.OracleDriver - (JDBC thin driver for Oracle 7 and 8 databases). When using OBBC-JDBC connection, you may use sun.jdbc.odbc.JdbcOdbcDriver.

Database Username

Enter the username used to login to the database.

Database Password

Enter a password used to login to the database.

Advanced Settings for the Concord Metrics Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Concord Metrics Monitor and its display in the product interface. Use this section to set monitor-to-monitor dependencies, customize display options, and configure other settings specific to the Concord Metrics Monitor that may be required in some infrastructure environments. Complete the entries as needed and click the **OK** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

EMS Configuration File Path

Enter the path to the EMS integration configuration file relative to the SiteScope installation. The default location is: <SiteScope root directory>\conf\ems\concord\metrics.config. For more information about the format of the file see the section "Integration Monitor Configuration Files" on page 1049.

If you want to edit this file, create a copy on the SiteScope machine and work in the new copy. Then, in Monitor Administration, edit the path to the file.

Maximum Number of Rows to Retrieve

Specify the maximum number of rows the monitor retrieves from the database for each monitor cycle. The default value is 5000.

If the number of result rows exceeds the set maximum, the monitor will retrieve the remaining rows (those that exceeded the maximum) on future cycles, until all result rows are retrieved.

The Max Rows value should be large enough to keep up with database table growth, yet small enough to avoid java.lang.OutOfMemoryException errors. Further, monitor run frequency should also be considered. Make sure that the rate at which data is collected by the monitor—which is dependent upon both monitor run frequency and network/system speed—is greater than or equal to the rate of data insertion on the monitored system.

SELECT

Enter an optional SELECT clause to be used in the SQL query. Enter * for all fields or a comma separated list of column names to be retrieved from the database. The default value for the Concord Metrics Monitor is *.

WHERE

Enter an optional WHERE clause to be used in the SQL query. This is an optional field which allows you to define the select criteria. Leaving it empty will result in retrieving all the rows from the table.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. You may, however, schedule your monitors to run only on certain days or on a fixed schedule. Click the Edit schedule link to create or edit a monitor schedule. For more information about working with monitor schedules, see the section on Schedule Preferences for Monitoring.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the other monitor should have for the current monitor to run normally. The current monitor will be run normally as long as the monitor selected in the **Depends On** field reports the condition selected in this field. For example, by selecting OK, this monitor is only enabled as long as the monitor selected in the **Depends On** field reports a status of good or OK.

Monitor Description

Enter additional information to describe this monitor. The Monitor Description can include HTML tags such as the <BR>, <HR>, and <B> tags to control display format and style. The description text will appear on the Monitor Detail page.

Report Description

Enter an optional description for this monitor that will make it easier to understand what the monitor does. For example, network traffic or main server response time. This description will be displayed on with each bar chart and graph in Management Reports and appended to the tool-tip displayed when you pass the mouse cursor over the status icon for this monitor on the Monitor Detail page.

EMS Time Difference

Use this option to account for time differences between the system clock time on the monitored EMS machine and the server where SiteScope is running. This is only needed when the EMS data includes time data and the time data shows that there is a time difference between the EMS machine and the SiteScope server. If the time difference is too great the data may be discarded from Mercury Business Availability Center.

Note: The time difference value only needs to be entered if the difference is greater than one minute. There is no need to synchronize differences of seconds less than one minute.

DB Machine Name

If you are reporting monitor data to an installation of Mercury Business Availability Center, enter a text identifier describing the database server that this monitor is monitoring. This text descriptor is used to identify the database server when the monitor data is viewed in a Mercury Business Availability Center report. Use only alphanumeric characters for this entry. You can enter the name of the monitored server or a description of the database that will be used to identify the host.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. When an error is detected, the monitor will immediately be scheduled to run again once.

Note: In order to change the run frequency of this monitor when an error is detected, you should use the **Error Frequency** option instead of the **Verify Error** option.

Note: The status returned by the **Verify Error** run of the monitor will replace the status of the originally scheduled run that detected an error. This may cause the loss of important performance data if the data from the verify run is different than the initial error status.

Use of this option across many monitor instances may result in significant monitoring delays in the case that multiple monitors are rescheduled to verify errors at the same time.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the status settings to set threshold conditions that determine the status of this Concord Metrics monitor instance based on the results returned by the check.

Each Concord Metrics monitor instance has three status settings:

- **Error if**
- **Warning if**
- **Good if**

While the monitor is enabled, it is assigned a status of good, warning, or error based on the most recent execution of the monitor action. The measurement taken or the results reported by the monitor are tested against the status threshold settings to determine the status. The status is displayed by color and a status icon in the SiteScope interface.

A change of status acts as a trigger for alerts associated with the monitor or the group to which the monitor belongs. For example, if the Concord Metrics Monitor detects that the Concord database for metrics has become unavailable, the status change from good to error is used to trigger an alert on error.

A change of status may also effect the state of a dependency between monitors.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement value. You may use the default status thresholds defined for the Concord Metrics or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop down menu to for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.

2 Use the second drop down menu to select the comparison operator(s) that will define the status threshold.

3 Enter a value applicable to the measurement parameter in the third text box.

4 Repeat these steps for the Warning if and Good if settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

109

HP OVO Event Monitor

The HP OVO Event Monitor allows you to integrate an existing Hewlett-Packard OpenView installation with Mercury Interactive's Mercury Business Availability Center by transferring HP OVO messages from HP OVO Server to a Mercury Business Availability Center server. This monitor supports HP OVO versions 6 and 7, when installed on Solaris 5.8 and later or installed on HP UX 11.x.

This chapter describes:	On page:
About the HP OVO Event Monitor	1147
Integration Architecture	1149
Working with the HP OVO Integration Add-on	1149
Configuring the HP OVO Event Monitor	1153

About the HP OVO Event Monitor

This monitor makes use of Mercury-supplied integration module that must be installed on the HP OpenView server.Once the HP OVO Event Monitor is configured and running, it collects events from HP OVO Server as these are created or modified, and transfers the events to the Mercury Business Availability Center.

The HP OVO Event monitor uses a pre-defined configuration file to define the processing of incoming data and define the output sample forwarded to Mercury Business Availability Center. If you have to make any specific customizations, you can modify this configuration file. For details, see “Integration Monitor Configuration Files” on page 1049.

Note: If you are upgrading SiteScope from version 7.8.1.2 or 7.9.0.0, see the note about upgrading Integration Monitor types for version 7.9.1.0 or later in the section "Working with SiteScope Integration Monitors" on page 1043.

Note: Hewlett Packard Network Node Manager data can be forwarded to Mercury Business Availability Center by using other Integration Monitors. See "Integration with HP Network Node Manager" on page 1325 for more information.

Operating Environment

The HP OVO Event Monitor depends on a Mercury Interactive HP OVO Integration Add-on to collect events from the HP OpenView Server. The Add-on, when installed on the HP OVO Server machine, listens to messages received by the HP OVO system and sends them to the HP OVO Event Monitor. The HP OVO Event Monitor transfers the messages to a Mercury Business Availability Center server. The Add-on and the monitor communicate using TCP/IP networking (using customizable TCP port).

Status

The status returned by the monitor is the current value of the monitor, such as 10 received alerts, 1 connected addon. The status is logged as either OK, warning, or error. A warning status is returned if no Add-on is connected to the monitor. The status can be configured further using advanced options in the HP OVO Alert Monitor Configuration Form.

Note: For information on Integration Monitor logging and troubleshooting, see "Integration Monitor Logging Options" on page 1046 and "Troubleshooting Integration Monitors" on page 1047.

Integration Architecture

HP OVO integration architecture is based on an add-on that listens to the HP OVO buses and forwards events using TCP protocol to the SiteScope HP OVO monitor. The HP OVO Integration Add-on listens to the following buses:

- **MSI bus** listens to newly created HP OVO events.
- **MSG bus** listens to updates on events such as acknowledge, close and owner events.

Working with the HP OVO Integration Add-on

The purpose of the HP OVO Integration Add-on is to connect to the HP OVO message infrastructure, to receive alerts from the HP OVO and to forward these alerts to the SiteScope machine.

Note: The Add-on module is platform specific. Currently we provide Add-on modules for the Solaris 8/9/SPARC and HP UX 11 platforms.

HP OVO Integration Installation

The following is an outline of the steps you use for the HP OVO Integration Installation Process:

1. Install and configure the HP OVO Integration Add-on on the HP OVO Server
2. Activate the HP OVO Event Monitor and the HP OVO Integration Add-on

   See the section Working with the HP OVO Integration Add-on below for more information about installing, activating, and configuring the Integration Add-on.

Detailed Add-on Installation Instructions

Following are the detailed installation instructions for the HP OVO Integration Add-on:

Before installing the HP OVO Integration Add-on

Prior to installation of the HP OVO Integration Add-on, make sure you have following data available:

- IP address (or network name) of the SiteScope machine on which the monitor is installed.
- Path to HP OVO server libraries (the default is /opt/OV/lib/)
- Path to the Oracle server software libraries.
- Path to the Java runtime libraries. For example, /usr/java1.1

Installing the HP OVO Integration Add-on

The HP OVO Integration Add-on is distributed as a .tar archive. You perform the following steps to install the Add-on:

1. Login as the super-user to the HP OVO Server; alternatively, use the `su` command to gain super-user permissions.
2. Choose an installation directory on the HP OVO Server. Create the directory if needed.

Note: It is highly recommended to install the Add-on under directory /opt/topaz/hp_ovo_addon/ as this minimizes the configuration changes needed.

---

3. If installing on the Solaris8 Platform, copy **<Sitescope root directory>\conf\ems\hp\addon\solaris\hp_mercury.solaris.tar** file to the installation directory. If installing on the HPUX 11 Platform, copy **<Sitescope root directory>\conf\ems\hp\addon\hpux\hp_mercury.hpux.tar** file to the installation directory.

4 Uncompress the tar file in the installation directory using the command: tar xvf hp_mercury.solaris.tar (this example is for the Solaris8 platform)

5 Configure the Add-on by editing the **run_addon.sh** file in the installation directory on the HP OVO Server. Refer to the configuration instruction section below for details.

Configuring the HP OVO Integration Add-on

Once installed, the Integration Add-on must be configured before it can be used. The configuration is done by editing the Add-on configuration script: `run_addon.sh`.

The following parameters must be set in the configuration file:

SIS_HOST

IP Address or network name of SiteScope machine on which the HP OVO Event Monitor is installed

OVO_DIR

Location of HP OVO server software libraries. (the default is: `/opt/OV/lib`)

JAVA_DIR

Location of Java software libraries (the default is: `/usr/java1.1/lib`)

ORACLE_DIR

Location of Oracle software libraries (the default is: /opt/oracle/product/8.1.7/lib)

In addition to these required parameters, following parameters can be customized:

PORT

TCP Port number for Addon-Monitor communication (default is 9000)

Note: If you change this setting, make sure to update the HP OVO Event Monitor.

LOG_DIR

Log directory. (default is `/tmp/hpovo_ito_addon`)

DEBUG_LEVEL

Debug level. Possible debug levels are: DEBUG/INFO/WARNING/ERROR (default is ERR0R).

LOG_FILE

Log file name. By default log file name is constructed automatically, based on the current date. You can override default behavior by setting explicit log file name here.

Uninstalling the Add-on from the HP OVO Server

If you must uninstall the Add-on files from the HP OVO server, perform the following procedure:

To remove the Add-on files from the HP OVO Server:

1. Log on as the superuser.
2. Make sure the Add-on is not running by executing the stop_addon.sh command.
3. Use the command: rm – rf <add-on directory> to completely remove the Add-on files.

Starting and Stopping the HP OVO Integration Add-on

The HP OVO Integration Add-on must be started using the `run_addon.sh` shell script, which comes with the package. It will connect to the HP OVO Event Monitor using the IP address specified in **run_addon.sh** shell script during the configuration.

Once started, the Add-on can be shut down using the termination script, **stop_addon.sh**.

If the Add-on disconnects from the SiteScope during operation, it will try to reconnect to the SiteScope at regular intervals. The events will be stored within the HP OVO software. In the case of add-on process termination, the messages will be held on the management server until the process can be brought up and then sent to Mercury Business Availability Center.

Configuring the HP OVO Event Monitor

The HP OVO Event Monitor should be added to a SiteScope monitor group created for this monitor and other Integration Monitor types. It is recommended that you configure Integrations Monitors only after a connection between the SiteScope and Mercury Business Availability Center is established.

Note: SiteScope cannot be deployed behind a firewall. The SiteScope and the monitored system must be on the same LAN or special firewall configuration may be required.

Main Settings for the HP OVO Event Monitor

You use the Main Settings section to specify the text name used for this monitor instance in the interface. Complete the entry in the Main Settings section as described below, and click the **OK** button to save the settings.

Name

Enter a text name for this HP OVO Event monitor instance. This text is displayed in the Monitor Administration interface and in the SiteScope interface. If you do not enter a name text, a default name will be used.

Advanced Settings for the HP OVO Event Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the HP OVO Event Monitor and its display in the product interface. Use this section to set monitor-to-monitor dependencies, customize display options, and configure other settings specific to the HP OVO Event Monitor that may be required in some infrastructure environments. Complete the entries as needed and click the **OK** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

EMS Configuration File Path

Enter the path to the EMS integration configuration file relative to the SiteScope installation. The default location is <SiteScope root directory>\conf\ems\hp\event.config. For more information about the format of the file see the section "Integration Monitor Configuration Files" on page 1049.

If you want to edit this file, create a copy on the SiteScope machine and work in the new copy. Then, in Monitor Administration, edit the path to the file.

Frequency

Select how often the monitor should update its status. The **Frequency** setting for the HP OVO Event Monitor controls only the status reports. The HP OVO system event data are forwarded when they are received without any delay. The default interval is to update once every 10 minutes. Use the drop-down list to the right of the text box to specify an update interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

HP OVO Add-on TCP Port

Enter the TCP port number as configured in the HP OVO Integration Add-on. By default port 9000 is used.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. You may, however, schedule your monitors to run only on certain days or on a fixed schedule. Click the Edit schedule link to create or edit a monitor schedule. For more information about working with monitor schedules, see the section on Schedule Preferences for Monitoring.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the other monitor should have for the current monitor to run normally. The current monitor will be run normally as long as the monitor selected in the **Depends On** field reports the condition selected in this field. For example, by selecting OK, this monitor is only enabled as long as the monitor selected in the **Depends On** field reports a status of good or OK.

Monitor Description

Enter additional information to describe this monitor. The Monitor Description can include HTML tags such as the <BR>, <HR>, and <B> tags to control display format and style. The description text will appear on the Monitor Detail page.

Report Description

Enter an optional description for this monitor that will make it easier to understand what the monitor does. For example, network traffic or main server response time. This description will be displayed on with each bar chart and graph in Management Reports and appended to the tool-tip displayed when you pass the mouse cursor over the status icon for this monitor on the Monitor Detail page.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. When an error is detected, the monitor will immediately be scheduled to run again once.

Note: In order to change the run frequency of this monitor when an error is detected, you should use the **Error Frequency** option instead of the **Verify Error** option.

Note: The status returned by the **Verify Error** run of the monitor will replace the status of the originally scheduled run that detected an error. This may cause the loss of important performance data if the data from the verify run is different than the initial error status.

Use of this option across many monitor instances may result in significant monitoring delays in the case that multiple monitors are rescheduled to verify errors at the same time.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the status settings to set threshold conditions that determine the status of this HP OVO Event monitor instance based on the results returned by the check.

Each HP OVO Event monitor instance has three status settings:

- **Error if**
- **Warning if**
- **Good if**

While the monitor is enabled, it is assigned a status of good, warning, or error based on the most recent execution of the monitor action. The measurement taken or the results reported by the monitor are tested against the status threshold settings to determine the status. The status is displayed by color and a status icon in the SiteScope interface.

A change of status acts as a trigger for alerts associated with the monitor or the group to which the monitor belongs. For example, if the HP OVO Event Monitor detects that the HP OVO system event data has become unavailable, the status change from good to error is used to trigger an alert on error.

A change of status may also effect the state of a dependency between monitors.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement value. You may use the default status thresholds defined for the HP OVO Event or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1 Use the first drop down menu to for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.

2 Use the second drop down menu to select the comparison operator(s) that will define the status threshold.

3 Enter a value applicable to the measurement parameter in the third text box.

4 Repeat these steps for the Warning if and Good if settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

110

HP SIM Event Monitor

The HP Systems Insight Manager Event Monitor watches for reports on health and availability of monitored devices arriving from HP Systems Insight Manager. It checks the results of a query for selected content and can alert you through Mercury Business Availability Center when certain entries are found.

This chapter describes:	On page:
About the HP SIM Event Monitor	1161
System Requirements	1162
Configuring the HP SIM Event Monitor	1163

About the HP SIM Event Monitor

The HP Systems Insight Manager Event Monitor watches for reports on health and availability of monitored devices arriving from HP Systems Insight Manager. It alerts you on any event reported by the HP Systems Insight Manager system.

Note: For information on Integration Monitor logging and troubleshooting, see Integration Monitor Logging Options and Troubleshooting Integration Monitors in Chapter 101, "Working with SiteScope Integration Monitors."

System Requirements

The following are requirements for using the HP Systems Insight Manager Event Monitor:

- You must use one of the database drivers supplied by default, or install or copy a compatible database driver or database access API into the appropriate SiteScope directory location. The supplied drivers include:

  com.inet.tds.TdsDriver - (TDS driver from i-net Software for Microsoft SQL databases)

  com.inet.ora.OraDriver - (JDBC thin driver for Oracle databases)

  Many other database driver packages are available as compressed (zipped) archive files or .jar files. Database drivers in this form must NOT be extracted and must be installed into the <SiteScope root directory>\java\lib\ext subdirectory.

- You need to know the syntax for the Database Connection URL. The Database Connection URL normally includes the class of driver you are using, some key name relating to the supplier of the driver software, followed by a combination of server, host, and port identifiers. Examples of database connection URLs are:

  jdbc:inetdae:hostname:port - (where hostname is the name of the host where the database is running and port is the port on which the database interfaces with the driver)

  jdbc:oracle:thin:@hostname:port:dbname - (where hostname is the name of the host where the database is running, port is the port on which the database interfaces with the driver, and dbname is the name of the Oracle database instance)

- The database you want to query must be running, have a database name defined, and have at least one named table created in the database. In some cases, the database management software needs to be configured to allow connections via the middleware or database driver.

- You need a valid username and password to access and perform a query on the database. In some cases, the machine and user account that SiteScope is running on must be given permissions to access the database.

The HP SIM Event monitor uses a pre-defined configuration file to define the processing of incoming data and define the output sample forwarded to Mercury Business Availability Center. If you have to make any specific customizations, you can modify this configuration file. For details, see "Integration Monitor Configuration Files" on page 1049.

Configuring the HP SIM Event Monitor

The HP SIM Event Monitor should be added to a SiteScope monitor group created for this monitor and other Integration Monitor types. It is recommended that you configure Integrations Monitors only after a connection between the SiteScope and Mercury Business Availability Center is established.

Note: SiteScope cannot be deployed behind a firewall. The SiteScope and the monitored system must be on the same LAN or special firewall configuration may be required.

Main Settings for the HP SIM Event Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the HP System Insight Manager system event data, how often this HP SIM Event Monitor instance should be run, and the text name used for this monitor instance in the interface. Complete the entries in the Main Settings section as described below. Complete the entries as needed and click the **OK** button to save the settings.

Name

Enter a text name for this HP SIM Event monitor instance. This text is displayed in the Monitor Administration interface and in the SiteScope interface. If you do not enter a name text, a default name will be used.

Frequency

Select how often the HP SIM Event monitor checks the database for events to forward to Mercury Business Availability Center. The default interval is to update once every 10 minutes. Use the drop-down list to the right of the text box to specify an update interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Database Connection URL

Enter a URL to a Database Connection (sometimes referred to as an Authentication string). One way to create a database connection is to use ODBC to create a named connection to a database. For example, first use the ODBC control panel to create a Data Source Name (DSN) called test under the system DSN tab. Then, enter jdbc:odbc:test in this box as the connection URL. Other way is to use the supplied MS SQL or Oracle driver in order to connect to the Database. When using the MS SQL driver, use the connection URL of the form jdbc:inetdae:<computer_name>:<port>?database=<db_name>. When using the Oracle driver, use the connection URL of the form jdbc:inetora:<computer_name>:<port>:<instance>.

Database Driver

Enter the driver used to connect to the database. Use the Fully Qualified Class Name of the JDBC driver you wish to use. The default drivers for this monitor are the com.inet.tds.TdsDriver - (TDS driver from i-net Software for Microsoft SQL databases) or oracle.jdbc.driver.OracleDriver - (JDBC thin driver for Oracle 7 and 8 databases). When using OBBC-JDBC connection, you may use sun.jdbc.odbc.JdbcOdbcDriver.

Database Username

Enter the username used to login to the database.

Database Password

Enter a password used to login to the database.

Advanced Settings for the HP SIM Event Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the HP SIM Event Monitor and its display in the product interface. Use this section to set monitor-to-monitor dependencies, customize display options, and configure other settings specific to the HP SIM Event Monitor that may be required in some infrastructure environments. Complete the entries as needed and click the **OK** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

EMS Configuration File Path

Enter the path to the EMS integration configuration file relative to the SiteScope installation. For more information about format of the file see EMS Configuration file format. The default location is: <SiteScope root directory>\conf\ems\hpsim\event.config. For more information about the format of the file see the section "Integration Monitor Configuration Files" on page 1049.

If you want to edit this file, create a copy on the SiteScope machine and work in the new copy. Then, in Monitor Administration, edit the path to the file.

Maximum Number of Rows to Retrieve

Specify the maximum number of rows the monitor retrieves from the database for each monitor cycle. The default value is 5000.

If the number of result rows exceeds the set maximum, the monitor will retrieve the remaining rows (those that exceeded the maximum) on future cycles, until all result rows are retrieved.

The Max Rows value should be large enough to keep up with database table growth, yet small enough to avoid java.lang.OutOfMemoryException errors. Further, monitor run frequency should also be considered. Make sure that the rate at which data is collected by the monitor—which is dependent upon both monitor run frequency and network/system speed—is greater than or equal to the rate of data insertion on the monitored system.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. You may, however, schedule your monitors to run only on certain days or on a fixed schedule. Click the Edit schedule link to create or edit a monitor schedule. For more information about working with monitor schedules, see the section on Schedule Preferences for Monitoring.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the other monitor should have for the current monitor to run normally. The current monitor will be run normally as long as the monitor selected in the **Depends On** field reports the condition selected in this field. For example, by selecting OK, this monitor is only enabled as long as the monitor selected in the **Depends On** field reports a status of good or OK.

Monitor Description

Enter additional information to describe this monitor. The Monitor Description can include HTML tags such as the <BR>, <HR>, and <B> tags to control display format and style. The description text will appear on the Monitor Detail page.

Report Description

Enter an optional description for this monitor that will make it easier to understand what the monitor does. For example, network traffic or main server response time. This description will be displayed on with each bar chart and graph in Management Reports and appended to the tool-tip displayed when you pass the mouse cursor over the status icon for this monitor on the Monitor Detail page.

EMS Time Difference

Use this option to account for time differences between the system clock time on the monitored EMS machine and the server where SiteScope is running. This is only needed when the EMS data includes time data and the time data shows that there is a time difference between the EMS machine and the SiteScope server. If the time difference is too great the data may be discarded from Mercury Business Availability Center.

Note: The time difference value only needs to be entered if the difference is greater than one minute. There is no need to synchronize differences of seconds less than one minute.

DB Machine Name

If you are reporting monitor data to an installation of Mercury Business Availability Center, enter a text identifier describing the database server that this monitor is monitoring. This text descriptor is used to identify the database server when the monitor data is viewed in a Mercury Business Availability Center report. Use only alphanumeric characters for this entry. You can enter the name of the monitored server or a description of the database that will be used to identify the host.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. When an error is detected, the monitor will immediately be scheduled to run again once.

Note: In order to change the run frequency of this monitor when an error is detected, you should use the **Error Frequency** option instead of the **Verify Error** option.

Note: The status returned by the **Verify Error** run of the monitor will replace the status of the originally scheduled run that detected an error. This may cause the loss of important performance data if the data from the verify run is different than the initial error status.

Use of this option across many monitor instances may result in significant monitoring delays in the case that multiple monitors are rescheduled to verify errors at the same time.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the status settings to set threshold conditions that determine the status of this HP SIM Event monitor instance based on the results returned by the check.

Each HP SIM Event monitor instance has three status settings:

- **Error if**
- **Warning if**
- **Good if**

While the monitor is enabled, it is assigned a status of good, warning, or error based on the most recent execution of the monitor action. The measurement taken or the results reported by the monitor are tested against the status threshold settings to determine the status. The status is displayed by color and a status icon in the SiteScope interface.

A change of status acts as a trigger for alerts associated with the monitor or the group to which the monitor belongs. For example, if the HP SIM Event Monitor detects that the HP System Insight Manager system event data has become unavailable, the status change from good to error is used to trigger an alert on error.

A change of status may also effect the state of a dependency between monitors.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement value. You may use the default status thresholds defined for the HP SIM Event or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop down menu to for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. Repeat these steps for the Warning if and Good if settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

111

Mercury Application Mapping Measurement Monitor

The Mercury Application Mapping Measurement Monitor is used to collect measurement information from the Mercury Application Mapping application and integrate this data with Mercury Business Availability Center.

This chapter describes:	On page:
About the Mercury Application Mapping Measurement Monitor	1173
Setup Requirements	1174
Configuring the Mercury Application Mapping Measurement Monitor	1175

About the Mercury Application Mapping Measurement Monitor

The Mercury Application Mapping Measurement Monitor watches for metrics from the Mercury Application Mapping database system and forwards the data to Dashboard and Business Availability Center. The monitor will create events (samples) for both the operation and change categories.

Note: For information on Integration Monitor logging and troubleshooting, see Integration Monitor Logging Options and Troubleshooting Integration Monitors in Chapter 101, "Working with SiteScope Integration Monitors."

Setup Requirements

The following are requirements for using the Mercury Application Mapping Measurement Monitor:

- The Mercury Application Mapping Measurement Monitor retrieves tickets from the Mercury Application Mapping system via a database connection. You must therefore have a working database driver installed on the SiteScope machine. SiteScope includes a default driver for use with this monitor.
- You need to know the syntax for accessing the database driver.
- You need to know the syntax for the Database Connection URL. The Database Connection URL normally includes the class of driver you are using, some key name relating to the supplier of the driver software, followed by a combination of server, host, and port identifiers.
- The Mercury Application Mapping database must be running. In some cases, the database management software needs to be configured to allow connections via the middleware or database driver.
- You need a valid username and password to access and perform a query on the Mercury Application Mapping database. In some cases, the machine and user account that SiteScope is running on must be given permissions to access the Mercury Application Mapping database.

The Mercury Application Mapping Measurement monitor uses a pre-defined configuration file to define the processing of incoming data and define the output sample forwarded to Mercury Business Availability Center. If you have to make any specific customizations, you can modify this configuration file. For details, see "Integration Monitor Configuration Files" on page 1049.

Configuring the Mercury Application Mapping Measurement Monitor

The Mercury Application Mapping Measurement Monitor can be added to any SiteScope monitor group container in the Enterprise tree. You configure the monitor using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings for the Mercury Application Mapping Measurement Monitor.

Main Settings for the Mercury Application Mapping Measurement Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the Mercury Application Mapping database, how often this Mercury Application Mapping Measurement Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this Mercury Application Mapping Measurement monitor instance. This text is displayed in the Monitor Administration interface and in the SiteScope interface. If you do not enter a name text, a default name will be used.

Frequency

Select how often the Mercury Application Mapping Measurement monitor checks the database for Mercury Application Mapping data to forward to Mercury Business Availability Center. The default interval is to update once every 10 minutes. Use the drop-down list to the right of the text box to specify an update interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Database Username

Enter the username used to login to the database.

Database Password

Enter a password used to login to the database.

Database Connection URL

Enter the URL to the Mercury Application Mapping Database Connection (sometimes referred to as an Authentication string). The default URL is, jdbc:inetora:hostname:port:instance where hostname is the name of the host where the database is running, port is the port on which the database interfaces with the driver and instance is the database instance that contains the mapping data.

Database Driver

Enter the driver used to connect to the database. Use the Fully Qualified Class Name of the database driver you wish to use. The default driver is the Oracle driver: com.inet.ora.OraDriver.

Advanced Settings for the Mercury Application Mapping Measurement Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Mercury Application Mapping Measurement Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

EMS Configuration File Path

Enter the path to the EMS integration configuration file. The default location is: <SiteScope root directory>\conf\ems\arm\event.config. For more information about the format of the file see the section "Integration Monitor Configuration Files" on page 1049.

Maximum Number of Rows to Retrieve

Specify the maximum number of rows the monitor retrieves from the database for each monitor cycle. The default value is 5000.

If the number of result rows exceeds the set maximum, the monitor will retrieve the remaining rows (those that exceeded the maximum) on future cycles, until all result rows are retrieved.

The Max Rows value should be large enough to keep up with database table growth, yet small enough to avoid java.lang.OutOfMemoryException errors. Further, monitor run frequency should also be considered. Make sure that the rate at which data is collected by the monitor—which is dependent upon both monitor run frequency and network/system speed—is greater than or equal to the rate of data insertion on the monitored system.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. You may, however, schedule your monitors to run only on certain days or on a fixed schedule. Click the Edit schedule link to create or edit a monitor schedule. For more information about working with monitor schedules, see the section on Schedule Preferences for Monitoring.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the other monitor should have for the current monitor to run normally. The current monitor will be run normally as long as the monitor selected in the **Depends On** field reports the condition selected in this field. For example, by selecting OK, this monitor is only enabled as long as the monitor selected in the **Depends On** field reports a status of good or OK.

Monitor Description

Enter additional information to describe this monitor. The Monitor Description can include HTML tags such as the <BR>, <HR>, and <B> tags to control display format and style. The description text will appear on the Monitor Detail page.

Report Description

Enter an optional description for this monitor that will make it easier to understand what the monitor does. For example, network traffic or main server response time. This description will be displayed on with each bar chart and graph in Management Reports and appended to the tool-tip displayed when you pass the mouse cursor over the status icon for this monitor on the Monitor Detail page.

EMS Time Difference

Use this option to account for time differences between the system clock time on the monitored EMS machine and the server where SiteScope is running. This is only needed when the EMS data includes time data and the time data shows that there is a time difference between the EMS machine and the SiteScope server. If the time difference is too great the data may be discarded from Mercury Business Availability Center.

Note: The time difference value only needs to be entered if the difference is greater than one minute. There is no need to synchronize differences of seconds less than one minute.

DB Machine Name

If you are reporting monitor data to an installation of Mercury Business Availability Center, enter a text identifier describing the database server that this monitor is monitoring. This text descriptor is used to identify the database server when the monitor data is viewed in a Mercury Business Availability Center report. Use only alphanumeric characters for this entry. You can enter the name of the monitored server or a description of the database that will be used to identify the host.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. When an error is detected, the monitor will immediately be scheduled to run again once.

Note: In order to change the run frequency of this monitor when an error is detected, you should use the **Error Frequency** option instead of the **Verify Error** option.

Note: The status returned by the **Verify Error** run of the monitor will replace the status of the originally scheduled run that detected an error. This may cause the loss of important performance data if the data from the verify run is different than the initial error status.

Use of this option across many monitor instances may result in significant monitoring delays in the case that multiple monitors are rescheduled to verify errors at the same time.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the status of this Mercury Application Mapping Measurement monitor instance based on the results returned by the check.

Each Mercury Application Mapping Measurement monitor instance has three status settings:

- **Error if**
- **Warning if**
- **Good if**

You can set unlimited threshold criteria for each status condition per Mercury Application Mapping Measurement monitor instance. By default, only one threshold is displayed when you first configure the monitor.

While the monitor is enabled, it is assigned a status of good, warning, or error based on the most recent execution of the monitor action. The measurement taken or the results reported by the monitor are tested against the status threshold settings to determine the status.

The individual results are combined as logical **OR** relationships when more than one threshold condition is defined for any of the three settings. When one or more of the conditions (for example when two conditions for **Error if** setting) are met for a status setting the monitor status is set to the corresponding status condition. If status conditions are met for more than one status setting the status of the monitor is set to the highest valued status condition. For example, if one condition selected as Error if and another condition selected as Warning if are both met, the status would be reported as an error, with **error** being the highest value, **warning** the next highest and **good** the lowest value. The status is displayed by color and a status icon in the SiteScope interface.

A change of status signals an event and acts as a trigger for alerts associated with the monitor or the group to which the monitor belongs.

A change of status may also effect the state of a dependency between monitors. For example, a monitor that detects a change that results in a error status may be a trigger to disable one or more other monitors that are dependent on the Mercury Application Mapping database.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement value. You may use the default status thresholds defined for the Mercury Application Mapping Measurement or use the following steps to change the monitor status thresholds for this monitor instance:

To edit monitor status thresholds:

1. Use the first drop down menu to for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

112

Netcool Event Monitor

The Netcool Event Monitor watches for alerts received from a Netcool server and forwards them to Mercury Business Availability Center. This provides a way to centralize data collection, to display data, and to alert you to conditions before they become serious. This monitor enables you to monitor Netcool 3.6 installed on any operating system.

This chapter describes:	On page:
About the Netcool Event Monitor	1185
Setup Requirements	1186
Configuring the Netcool Event Monitor	1187

About the Netcool Event Monitor

The Netcool Event Monitor is designed to collect SNMP Trap data from Netcool servers. Each time that the monitor is run, SiteScope checks traps that have been received since the last time the monitor ran and reports the results to Mercury Business Availability Center.

Note: For information on Integration Monitor logging and troubleshooting, see "Integration Monitor Logging Options" on page 1046 and "Troubleshooting Integration Monitors" on page 1047.

Note: If you are upgrading SiteScope from version 7.8.1.2 or 7.9.0.0, see the note about upgrading Integration Monitor types for version 7.9.1.0 or later in the section "Working with SiteScope Integration Monitors" on page 1043.

Setup Requirements

The following are requirements for using the Netcool Event Monitor to forward alerts to Mercury Business Availability Center:

- The Netcool server needs to be configured to send traps to the SiteScope server.

Note: The Netcool Event Monitor uses port 162 for receiving traps. If another application or process on the machine where SiteScope is running has bound this port, the monitor will report an "Address in use" error and the monitor type will be unavailable.

- SiteScope must be registered with a Business Availability Center installation. The SiteScope must have a profile defined in the Business Availability Center installation prior to enabling the registration in the SiteScope interface. In order to verify registration or to re-register SiteScope with the Business Availability Center server, see the Mercury Business Availability Center Registration page under SiteScope Preferences.
- The Netcool Event Monitor must be set to synchronize EMS data with Mercury Business Availability Center. See the Completing the Netcool Event Monitor Form section below for more information.

  The Netcool Event monitor uses a pre-defined configuration file to define the processing of incoming data and define the output sample forwarded to Mercury Business Availability Center. If you have to make any specific customizations, you can modify this configuration file. For details, see "Integration Monitor Configuration Files" on page 1049.

Configuring the Netcool Event Monitor

The Netcool Event Monitor should be added to a SiteScope monitor group created for this monitor and other Integration Monitor types. It is recommended that you configure Integrations Monitors only after a connection between the SiteScope and Mercury Business Availability Center is established.

Note: SiteScope cannot be deployed behind a firewall. The SiteScope and the monitored system must be on the same LAN or special firewall configuration may be required.

Main Settings for the Netcool Event Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the Netcool event data, how often this Netcool Event Monitor instance should be run, and the text name used for this monitor instance in the interface. Complete the entries in the Main Settings section as described below. Complete the entries as needed and click the **OK** button to save the settings.

Name

Enter a text name for this Netcool Event monitor instance. This text is displayed in the Monitor Administration interface and in the SiteScope interface. If you do not enter a name text, a default name will be used.

Advanced Settings for the Netcool Event Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Netcool Event Monitor and its display in the product interface. Use this section to set monitor-to-monitor dependencies, customize display options, and configure other settings specific to the Netcool Event Monitor that may be required in some infrastructure environments. Complete the entries as needed and click the **OK** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

EMS Configuration File Path

Enter the path to the EMS integration configuration file relative to the SiteScope installation. The default location is: <SiteScope root directory>\conf\ems\netcool\event.config. For more information about the format of the file see the section "Integration Monitor Configuration Files" on page 1049.

If you want to edit this file, create a copy on the SiteScope machine and work in the new copy. Then, in Monitor Administration, edit the path to the file.

Frequency

Select how often the monitor should update its status. The **Frequency** setting for the Netcool Event Monitor controls only the status reports. The Netcool event data are forwarded when they are received without any delay. The default interval is to update once every 10 minutes. Use the drop-down list to the right of the text box to specify an update interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Run Alerts

Choose the method for running alerts. If "for each event received from Netcool system " is chosen, then the monitor triggers alerts for every matching entry found.

Note: When the Netcool Event Monitor is run in the "for each event received from Netcool system" alert method, the monitor will never report a status of error or warning, regardless of the results of the content match or even if the target SNMP Trap is not found.

If the "once, after all events from Netcool system were received" method is chosen, then the monitor counts up the number of matches and triggers alerts based on the **Error if** and **Warning if** thresholds defined for the monitor in the Threshold Setting section.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. You may, however, schedule your monitors to run only on certain days or on a fixed schedule. Click the Edit schedule link to create or edit a monitor schedule. For more information about working with monitor schedules, see the section on Schedule Preferences for Monitoring.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the other monitor should have for the current monitor to run normally. The current monitor will be run normally as long as the monitor selected in the **Depends On** field reports the condition selected in this field. For example, by selecting OK, this monitor is only enabled as long as the monitor selected in the **Depends On** field reports a status of good or OK.

Monitor Description

Enter additional information to describe this monitor. The Monitor Description can include HTML tags such as the <BR>, <HR>, and <B> tags to control display format and style. The description text will appear on the Monitor Detail page.

Report Description

Enter an optional description for this monitor that will make it easier to understand what the monitor does. For example, network traffic or main server response time. This description will be displayed on with each bar chart and graph in Management Reports and appended to the tool-tip displayed when you pass the mouse cursor over the status icon for this monitor on the Monitor Detail page.

EMS Time Difference

Use this option to account for time differences between the system clock time on the monitored EMS machine and the server where SiteScope is running. This is only needed when the EMS data includes time data and the time data shows that there is a time difference between the EMS machine and the SiteScope server. If the time difference is too great the data may be discarded from Mercury Business Availability Center.

Note: The time difference value only needs to be entered if the difference is greater than one minute. There is no need to synchronize differences of seconds less than one minute.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. When an error is detected, the monitor will immediately be scheduled to run again once.

Note: In order to change the run frequency of this monitor when an error is detected, you should use the **Error Frequency** option instead of the **Verify Error** option.

Note: The status returned by the **Verify Error** run of the monitor will replace the status of the originally scheduled run that detected an error. This may cause the loss of important performance data if the data from the verify run is different than the initial error status.

Use of this option across many monitor instances may result in significant monitoring delays in the case that multiple monitors are rescheduled to verify errors at the same time.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely

- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the status of this Netcool Event monitor instance based on the results returned by the check.

Each Netcool Event monitor instance has three status settings:

- **Error if**
- **Warning if**
- **Good if**

You can set unlimited threshold criteria for each status condition per Netcool Event monitor instance. By default, only one threshold is displayed when you first configure the monitor.

While the monitor is enabled, it is assigned a status of good, warning, or error based on the most recent execution of the monitor action. The measurement taken or the results reported by the monitor are tested against the status threshold settings to determine the status.

The individual results are combined as logical **OR** relationships when more than one threshold condition is defined for any of the three settings. When one or more of the conditions (for example when two conditions for **Error if** setting) are met for a status setting the monitor status is set to the corresponding status condition. If status conditions are met for more than one status setting the status of the monitor is set to the highest valued status condition. For example, if one condition selected as Error if and another condition selected as Warning if are both met, the status would be reported as an error, with **error** being the highest value, **warning** the next highest and **good** the lowest value. The status is displayed by color and a status icon in the SiteScope interface.

A change of status signals an event and acts as a trigger for alerts associated with the monitor or the group to which the monitor belongs.

A change of status may also effect the state of a dependency between monitors. For example, a monitor that detects a change that results in a error status may be a trigger to disable one or more other monitors that are dependent on the Netcool event data.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement value. You may use the default status thresholds defined for the Netcool Event or use the following steps to change the monitor status thresholds for this monitor instance:

To edit monitor status thresholds:

1. Use the first drop down menu to for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.

4 To add another threshold setting, click the **New Error If** button and repeat the steps above.

5 Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

113

NetIQ Metrics Monitor

The NetIQ Metrics Monitor allows you to collect data from NetIQ database and forward it to Mercury Business Availability Center as SiteScope metrics. This monitor enables you to monitor NetIQ versions 5.0 and 5.1 installed on any operating system.

This chapter describes:	On page:
About the NetIQ Metrics Monitor	1195
Configuring the NetIQ Metrics Monitor	1197
NetIQ Integration with EMS Metrics	1206

About the NetIQ Metrics Monitor

The following are system requirements for configuring and using the NetIQ Metrics Monitor:

- You must use one of the database drivers supplied by default, or install or copy a compatible database driver or database access API into the appropriate SiteScope directory location. The supplied drivers include:

  com.inet.tds.TdsDriver - (TDS driver from i-net Software for Microsoft SQL databases)

  com.inet.ora.OraDriver - (JDBC thin driver for Oracle databases)

  Many other database driver packages are available as compressed (zipped) archive files or .jar files. Database drivers in this form must NOT be extracted and must be installed into the <SiteScope root directory>/java/lib/ext subdirectory.

Note: The sun JDBC:ODBC (sun.jdbc.odbc.JdbcOdbcDriver) driver is no longer supported by this monitor. It is recommended to use the JDBC driver supplied with SiteScope (com.inet.tds.TdsDriver).

- You need to know the syntax for the Database Connection URL. The Database Connection URL normally includes the class of driver you are using, some key name relating to the supplier of the driver software, followed by a combination of server, host, and port identifiers. Examples of database connection URL's are:

  jdbc:inetdae:<hostname>:<port>?database=<dbname> - (where hostname is the name of the host where the database is running and port is the port on which the database interfaces with the driver)

- The NetIQ repository you want to query must be running.
- You need a valid username and password to access and perform a query on the database.

The NetIQ Metrics monitor uses a pre-defined configuration file to define the processing of incoming data and define the output sample forwarded to Mercury Business Availability Center. If you have to make any specific customizations, you can modify this configuration file. For details, see "Integration Monitor Configuration Files" on page 1049.

Note: For information on Integration Monitor logging and troubleshooting, see "Integration Monitor Logging Options" on page 1046 and "Troubleshooting Integration Monitors" on page 1047.

Note: If you are upgrading SiteScope from version 7.8.1.2 or 7.9.0.0, see the note about upgrading Integration Monitor types for version 7.9.1.0 or later in the section "Working with SiteScope Integration Monitors" on page 1043.

Topology File

It is recommended that you create a topology file before you configure the NetIQ Metrics Monitor. You use a topology file to limit the data collected by the NetIQ Metrics Monitor to a subset of the servers being monitored by the NetIQ system. You use the following steps and command line tools located at <SiteScope root directory>\conf\ems\NetIQ folder in order to create the topology file.

To create a topology file:

1. Open the ConnectionDetails.xml file using a text editor. The file is found in the <SiteScope root directory>\conf\ems\NetIQ folder.
2. Edit the file to add the correct connection details. For example:

```
<NetIQ>
<connection password="pwd" user="usr" driverClass="com.inet.tds.TdsDriver"
url=" jdbc:inetdae:<host>:<port>?database=QDB"/>
```

3. Save the changes to the file.
4. Run the batch file importNetIQ.bat
5. Open the ConnectionDetails.xml file again and remove the servers you want to filter out.
6. Run the batch file filterNetIQ.bat. This should create a file named tpntq.xml.
7. Open the ConnectionDetails.xml file again and delete the authorization credentials from the file (for security). Save the file.

Configuring the NetIQ Metrics Monitor

The NetIQ Metrics Monitor should be added to a SiteScope monitor group created for this monitor and other Integration Monitor types. It is recommended that you configure Integrations Monitors only after a connection between the SiteScope and Mercury Business Availability Center is established.

Note: SiteScope cannot be deployed behind a firewall. The SiteScope and the monitored system must be on the same LAN or special firewall configuration may be required.

Main Settings for the NetIQ Metrics Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the NetIQ database for metrics, how often this NetIQ Metrics Monitor instance should be run, and the text name used for this monitor instance in the interface. Complete the entries in the Main Settings section as described below. Complete the entries as needed and click the **OK** button to save the settings.

Name

Enter a text name for this NetIQ Metrics monitor instance. This text is displayed in the Monitor Administration interface and in the SiteScope interface. If you do not enter a name text, a default name will be used.

Frequency

Select how often the monitor should update its status. The **Frequency** setting for the NetIQ Metrics Monitor controls only the status reports. The NetIQ database for metrics are forwarded when they are received without any delay. The default interval is to update once every 10 minutes. Use the drop-down list to the right of the text box to specify an update interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Database Connection URL

Enter a URL to a Database Connection (sometimes referred to as an Authentication string). One way to create a database connection is to use ODBC to create a named connection to a database. For example, first use the ODBC control panel to create a Data Source Name (DSN) called test under the system DSN tab. Then, enter jdbc:odbc:test in this box as the connection URL. Other way is to use the supplied MS SQL or Oracle driver in order to connect to the Database. When using the MS SQL driver, use the connection URL of the form jdbc:inetdae:<computer_name>:<port>?database=<db_name>. When using the Oracle driver, use the connection URL of the form jdbc:inetora:<computer_name>:<port>:<instance>.

Database Driver

Enter the driver used to connect to the database. Use the Fully Qualified Class Name of the JDBC driver you wish to use. The default drivers for this monitor are the com.inet.tds.TdsDriver - (TDS driver from i-net Software for Microsoft SQL databases) or oracle.jdbc.driver.OracleDriver - (JDBC thin driver for Oracle 7 and 8 databases). When using OBBC-JDBC connection, you may use sun.jdbc.odbc.JdbcOdbcDriver.

Database Username

Enter the username used to login to the database.

Database Password

Enter a password used to login to the database

Topology File Path

The path to the file on the SiteScope machine that define the topology of the system monitored by the NetIQ system. The monitor uses the configuration defined in the file to filter the metrics that is sends to Mercury Business Availability Center. If the file does not exist the monitor will create new file reflecting the configuration defined in the Master view of NetIQ.

Advanced Settings for the NetIQ Metrics Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the NetIQ Metrics Monitor and its display in the product interface. Use this section to set monitor-to-monitor dependencies, customize display options, and configure other settings specific to the NetIQ Metrics Monitor that may be required in some infrastructure environments. Complete the entries as needed and click the **OK** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

EMS Configuration File Path

Enter the path to the EMS integration configuration file relative to the SiteScope installation. The default location is: <SiteScope root directory>\conf\ems\netiq\metrics.config. For more information about the format of the file see the section "Integration Monitor Configuration Files" on page 1049.

If you want to edit this file, create a copy on the SiteScope machine and work in the new copy. Then, in Monitor Administration, edit the path to the file.

Maximum Number of Rows to Retrieve

Specify the maximum number of rows the monitor retrieves from the database for each monitor cycle. The default value is 5000.

If the number of result rows exceeds the set maximum, the monitor will retrieve the remaining rows (those that exceeded the maximum) on future cycles, until all result rows are retrieved.

The Max Rows value should be large enough to keep up with database table growth, yet small enough to avoid java.lang.OutOfMemoryException errors. Further, monitor run frequency should also be considered. Make sure that the rate at which data is collected by the monitor—which is dependent upon both monitor run frequency and network/system speed—is greater than or equal to the rate of data insertion on the monitored system.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. You may, however, schedule your monitors to run only on certain days or on a fixed schedule. Click the Edit schedule link to create or edit a monitor schedule. For more information about working with monitor schedules, see the section on Schedule Preferences for Monitoring.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the other monitor should have for the current monitor to run normally. The current monitor will be run normally as long as the monitor selected in the **Depends On** field reports the condition selected in this field. For example, by selecting OK, this monitor is only enabled as long as the monitor selected in the **Depends On** field reports a status of good or OK.

Monitor Description

Enter additional information to describe this monitor. The Monitor Description can include HTML tags such as the <BR>, <HR>, and <B> tags to control display format and style. The description text will appear on the Monitor Detail page.

Report Description

Enter an optional description for this monitor that will make it easier to understand what the monitor does. For example, network traffic or main server response time. This description will be displayed on with each bar chart and graph in Management Reports and appended to the tool-tip displayed when you pass the mouse cursor over the status icon for this monitor on the Monitor Detail page.

EMS Time Difference

Use this option to account for time differences between the system clock time on the monitored EMS machine and the server where SiteScope is running. This is only needed when the EMS data includes time data and the time data shows that there is a time difference between the EMS machine and the SiteScope server. If the time difference is too great the data may be discarded from Mercury Business Availability Center.

Note: The time difference value only needs to be entered if the difference is greater than one minute. There is no need to synchronize differences of seconds less than one minute.

DB Machine Name

If you are reporting monitor data to an installation of Mercury Business Availability Center, enter a text identifier describing the database server that this monitor is monitoring. This text descriptor is used to identify the database server when the monitor data is viewed in a Mercury Business Availability Center report. Use only alphanumeric characters for this entry. You can enter the name of the monitored server or a description of the database that will be used to identify the host.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. When an error is detected, the monitor will immediately be scheduled to run again once.

Note: In order to change the run frequency of this monitor when an error is detected, you should use the **Error Frequency** option instead of the **Verify Error** option.

Note: The status returned by the **Verify Error** run of the monitor will replace the status of the originally scheduled run that detected an error. This may cause the loss of important performance data if the data from the verify run is different than the initial error status.

Use of this option across many monitor instances may result in significant monitoring delays in the case that multiple monitors are rescheduled to verify errors at the same time.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the status settings to set threshold conditions that determine the status of this NetIQ Metrics monitor instance based on the results returned by the check.

Each NetIQ Metrics monitor instance has three status settings:

- **Error if**
- **Warning if**
- **Good if**

While the monitor is enabled, it is assigned a status of good, warning, or error based on the most recent execution of the monitor action. The measurement taken or the results reported by the monitor are tested against the status threshold settings to determine the status. The status is displayed by color and a status icon in the SiteScope interface.

A change of status acts as a trigger for alerts associated with the monitor or the group to which the monitor belongs. For example, if the NetIQ Metrics Monitor detects that the NetIQ database for metrics has become unavailable, the status change from good to error is used to trigger an alert on error.

A change of status may also effect the state of a dependency between monitors.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement value. You may use the default status thresholds defined for the NetIQ Metrics or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop down menu to for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. Repeat these steps for the Warning if and Good if settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

NetIQ Integration with EMS Metrics

EMS metrics integration does not support quality per EMS metric. To enable monitoring quality per metric, you must add more matching sections to the default NetIQ **metrics.config** file found in the **<SiteScope root directory>\conf\ems\netiq** directory. The additional sections can set different values for the Quality field according to a matching condition. For example:

```
$MATCH=$shortDesc.matches("Counter value for System NT_MemUtil.Avail")
&& parseDouble($value)>parseDouble("0.0")
```

You must write each additional section all on one line.

114

Remedy Ticketing Monitor

The Remedy Ticketing Monitor watches for “Interesting Tickets” received from Remedy Action Request System, versions 5.x and 6.0. Use this monitor to bring “Interesting Tickets” from a Remedy system to Mercury Business Availability Center. This monitor enables you to monitor Remedy Help Desk versions 5.x and 6.0 installed on any operating system.

This chapter describes:	On page:
About Remedy System Terminology	1207
About the Remedy Ticketing Monitor	1208
Software Requirements	1209
Remedy HelpDesk Integration Options for SiteScope	1211
Configuring the Remedy Ticketing Monitor	1214

About Remedy System Terminology

Remedy System

Remedy Action Request System is Remedy's application platform and development environment for delivering Service Management solutions. Remedy is a request-centric development and delivery platform used to create applications for entering, tracking, and resolving service requests. The SiteScope Monitor supports Remedy Server version 5.x and 6.0.

Remedy Help Desk

Remedy Help Desk leverages Remedy's Action Request System. It automates support processes including the ability to submit, monitor, and manage help desk cases, change requests, and asset inventory records.

Interesting Tickets

HelpDesk cases that are defined by the user as "interesting" (tickets with that do not have a "Closed" status by default).

About the Remedy Ticketing Monitor

Remedy Ticketing Monitor requires Remedy Action Request System version 5.x and 6.0 with the standard or customized HelpDesk application.

Note: The Remedy Ticketing Monitor is currently only supported for Microsoft Windows platforms.

Remedy Ticketing Monitor is useful for automatically collecting "Interesting Tickets" from Remedy Action Request System. HelpDesk cases are considered to be "interesting" according to definitions set by the user. Using SiteScope to collect ticket information automatically eliminates the need to check for the open tickets manually. In addition, you can be notified of any change in the existing HelpDesk tickets that you might have otherwise been unaware unless you check the Remedy client UI. Each time the monitor is run, it checks the Open Tickets currently on the Remedy system.

The Remedy Ticketing monitor uses a pre-defined configuration file to define the processing of incoming data and define the output sample forwarded to Mercury Business Availability Center. If you have to make any specific customizations, you can modify this configuration file. For details, see “Integration Monitor Configuration Files” on page 1049.

Note: For information on Integration Monitor logging and troubleshooting, see "Integration Monitor Logging Options" on page 1046 and "Troubleshooting Integration Monitors" on page 1047.

Note: If you are upgrading SiteScope from version 7.8.1.2 or 7.9.0.0, see the note about upgrading Integration Monitor types for version 7.9.1.0 or later in the section "Working with SiteScope Integration Monitors" on page 1043.

Software Requirements

Before you can use the Remedy Ticketing Monitor, you must copy several Remedy software libraries into the SiteScope installation path. Use the following steps to copy the applicable software files to the folders indicated. The dll names listed are relevant when using Remedy version 5.1.

Note: It is not necessary for the Remedy installation on the SiteScope machine to be used as a production system. The user will not have to run this server, but he must have a license to do so. Full installation of the Remedy Server is not mandatory to enable the Remedy Ticketing Monitor. You may simply copy the necessary files as described below as long as you follow the terms of your Remedy licensing agreement.

- Install the Remedy Server software on the machine where SiteScope is running.
- Copy all the files from the **<Remedy root directory>\ARserver\Api\lib** folder to the **SiteScope\WEB-INF\lib** folder.
- Also copy all the files from the same **<Remedy root directory>\ARserver\Api\lib** folder to the **SiteScope\bin** folder.

- Copy the file **<Remedy root directory>\arrpc51.dll** to the **SiteScope\bin** folder.
- Copy the file **<Remedy root directory>\arutl51.dll** to the **SiteScope\bin** folder.
- Stop and restart the SiteScope service.

Working with a Customized Remedy HelpDesk

If you are using a customized Remedy HelpDesk application, you need to do the following steps to configure the Remedy Ticketing monitor to work with it. Consult with your Remedy administrator for more information:

To configure the Remedy Ticketing Monitor for customized Remedy systems:

1. Make a copy of the <SiteScope root directory>\conf\ems\remedy\Remedy.def file and rename it to another file name (for example, CustomRemedy.def).
2. Edit the file you created using a text editor. The original definition file contains field names and values that correspond to the standard Remedy HelpDesk application. For the meaning of the fields, look at the standard HelpDesk application. You need to change only the values on the right side of each name-value pair as follows:

   Change the "Form", "Schema", and other fields under the "Assets" and "HelpDesk" sections according to the definition of your custom Remedy application. You must fill all required fields. The original definition contains the field names and values that correspond to the standard Remedy HelpDesk application. Do not delete any section from the file.
3. The "Association" section defines the fields that create a ticket-asset association. Change the values of those fields according to the appropriate Remedy ticket-asset association form.
4. Change the value entered for the **Remedy Schema Definition File** field in the monitor definition form according to the chosen file name. From this example the file name would become `CustomRemedy.def`.
5. Edit the **Interesting Ticket Query** entry in the monitor definition form. Replace the "Status" and "Resolved" values with the appropriate values from the customized Remedy application.

6 Restart the SiteScope service.

7 If you've installed the optional Mercury Notify addon component on the Remedy server, you need to edit the filter definition using the following steps:

8 Attach the filter to the correct customized HelpDesk form instead of the standard HPD:HelpDesk.

9 Replace the "Case ID+" field (under the If Action->Command Line) with the customized ticket ID field name.

Remedy HelpDesk Integration Options for SiteScope

There are two options that can be used for SiteScope to get the status of tickets from the Remedy HelpDesk System. The two options are:

- Configure SiteScope to query the Remedy host at regular intervals for Remedy tickets. You use the Remedy Ticketing Monitor for this option. Complete the applicable settings in the Add Remedy Ticketing Monitor form as described below. This is the recommended working mode.
- Configure the Remedy Server to send any HelpDesk ticket changes directly to SiteScope. This option requires that you make configuration changes and install a ticket notification module on the Remedy server. See the section Configuring the Remedy Addon to Send Ticket Information to SiteScope below for more information on this option.

  You can also configure SiteScope to forward ticket content information to Mercury Business Availability Center. The section Forwarding Ticket Content Information to Mercury Business Availability Center below describes an overview of how to configure the Remedy Ticketing Monitor for this option.

Sending Ticket Information to SiteScope

You can configure the Remedy server to send ticket change information directly to SiteScope. To enable this option, you must edit a configuration file and install a notification module on the Remedy server. Use the following steps to enable this option.

To configure the Remedy Server to send HelpDesk Ticket changes to the SiteScope machine:

Unpack the installation zip file

1 Extract the files contained in the `remedy_mercury.zip` file (located in the <SiteScope root directory>\conf\ems\remedy\addon directory) to a temporary directory.

Configure the `remedy_mercury_notify` Remedy Server Object

1 Open the file `remedy_mercury_notify.def` with a text editor

2 Replace the parameters in the line starting with the string `command` with values applicable to your installation environment. Parameters will appear between < > bracket delimiters.

Replace the following parameters with the values that describe your installation environment as follows:

<Remedy Installation Folder> - Replace this with the full path location to where the Remedy Server is installed relative to the machine where Remedy is installed. For example, `C:\Program Files\Remedy`.

<SiteScopeMachineName> - Replace this with the name of the machine where SiteScope is installed. This string can be the machine name, or the IP address.

<SiteScopePort=8888> - Replace this with the port number that SiteScope uses to listen for Remedy notifications. By default it is configured to listen on port 8888, but you must specify this value.

Note: Do not edit other parameters in the file. All others parameters should remain as originally defined

---

3 Save the changes to the file.

Install the notify package

Note: You must have a Remedy administrator privileges in order to install the **notify** package in the Remedy Server environment. Contact your Remedy System or network administrator, if necessary, to access the correct privileges.

To install the notify package:

1. Copy the file remedy_mercury.exe that is part of the `remedy_mercury.zip` package to the Remedy installation directory. For example, copy the file to: C:\Program Files\Remedy.
2. Verify that the Action Request Service is running and login to the Remedy Administrator.
3. Select the Remedy Server from the **Servers** tree, and choose to import definitions from a definition file (Tools > Import Definitions > From Definition File).
4. Select the file remedy_mercury_notify.def that you modified and saved in the above section b above.
5. From the Import Definitions Dialog, click **Add All**, and then click **Import**. **Note:** This operation may take several minutes.
6. When the import operation is complete close the Dialog Box
7. In the **Servers** tree, double-click to open the server's list of objects and verify that on the **Filters** object list, there is a filter named: Mercury_Notify. Use the right-pane of the **Filters** objects to navigate to find the object by this name.
8. Exit from the Remedy Administrator.

Forwarding Ticket Content Information to Mercury Business Availability Center

When forwarding the "Interesting Tickets", SiteScope can analyze the information within the Ticket and process it for Mercury Business Availability Center. The processing can be configured using the applicable EMS Configuration file. You specify the path to the EMS Configuration file relative to the SiteScope installation using **EMS Configuration File Path** field in the Advanced Settings section. See the section on “Integration Monitor Configuration Files” on page 1049 for more details on the file structure and syntax.

Note: Only tickets that are attached to assets will be counted by the monitor as "interesting" and forwarded to the Mercury Business Availability Center.

Configuring the Remedy Ticketing Monitor

The Remedy Ticketing Monitor should be added to a SiteScope monitor group created for this monitor and other Integration Monitor types. It is recommended that you configure Integrations Monitors only after a connection between the SiteScope and Mercury Business Availability Center is established.

Note: SiteScope cannot be deployed behind a firewall. The SiteScope and the monitored system must be on the same LAN or special firewall configuration may be required.

Main Settings for the Remedy Ticketing Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the Remedy Action Request System for ticket information, how often this Remedy Ticketing Monitor instance should be run, and the text name used for this monitor instance in the interface. Complete the entries in the Main Settings section as described below. Complete the entries as needed and click the **OK** button to save the settings.

Name

Enter a text name for this Remedy Ticketing monitor instance. This text is displayed in the Monitor Administration interface and in the SiteScope interface. If you do not enter a name text, a default name will be used.

Frequency

Select how often the monitor should update its status. The **Frequency** setting for the Remedy Ticketing Monitor controls only the status reports. The Remedy Action Request System for ticket information are forwarded when they are received without any delay. The default interval is to update once every 10 minutes. Use the drop-down list to the right of the text box to specify an update interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Remedy Server Name

Enter the name or the IP of the Remedy server host to connect to. The Remedy Server should be of version 5.x and 6.0.

Remedy User Name

Enter a valid user name that will be used to connect to the above Remedy Server.

Note: The user have to be a valid user name in the Remedy Server application with "read" permission at least for retrieving the tickets details from the HelpDesk schema.

Remedy Password

Enter the password of the above user name for a valid connection to the server.

Remedy Schema Definition File

Insert the path for the file that describes the Remedy schema definitions. By default the installation supplies the file: Remedy.def located under <SiteScope root directory>\conf\ems\remedy directory. See the Configuring the Remedy Ticketing Monitor section below for more details.

Interesting Tickets Query

Enter the Remedy user query that will be used as the filter to match the "Interesting Tickets". If you do not set this, SiteScope will use the default query string 'Status'<="Resolved".

Note: The syntax to write such a query is the same syntax as appeared in the Remedy Advanced Search dialog at the Remedy Support client tool. Please consult Remedy's User Guide help for any assistance in creating such queries.

Advanced Settings for the Remedy Ticketing Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Remedy Ticketing Monitor and its display in the product interface. Use this section to set monitor-to-monitor dependencies, customize display options, and configure other settings specific to the Remedy Ticketing Monitor that may be required in some infrastructure environments. Complete the entries as needed and click the **OK** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

EMS Configuration File Path

Enter the full path to the alternative EMS configuration file relative to the SiteScope installation. If you do not set the path, SiteScope will use a default path which is <SiteScope root directory>\conf\ems\remedy\event.config. You do not need to edit this file unless you change the meaning of the required Remedy fields in the Remedy Schema Definition file. For more information about the format of the file see the section "Integration Monitor Configuration Files" on page 1049.

If you want to edit this file, create a copy on the SiteScope machine and work in the new copy. Then, in Monitor Administration, edit the path to the file.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. You may, however, schedule your monitors to run only on certain days or on a fixed schedule. Click the Edit schedule link to create or edit a monitor schedule. For more information about working with monitor schedules, see the section on Schedule Preferences for Monitoring.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the other monitor should have for the current monitor to run normally. The current monitor will be run normally as long as the monitor selected in the **Depends On** field reports the condition selected in this field. For example, by selecting OK, this monitor is only enabled as long as the monitor selected in the **Depends On** field reports a status of good or OK.

Monitor Description

Enter additional information to describe this monitor. The Monitor Description can include HTML tags such as the <BR>, <HR>, and <B> tags to control display format and style. The description text will appear on the Monitor Detail page.

Report Description

Enter an optional description for this monitor that will make it easier to understand what the monitor does. For example, network traffic or main server response time. This description will be displayed on with each bar chart and graph in Management Reports and appended to the tool-tip displayed when you pass the mouse cursor over the status icon for this monitor on the Monitor Detail page.

EMS Time Difference

Use this option to account for time differences between the system clock time on the monitored EMS machine and the server where SiteScope is running. This is only needed when the EMS data includes time data and the time data shows that there is a time difference between the EMS machine and the SiteScope server. If the time difference is too great the data may be discarded from Mercury Business Availability Center.

Note: The time difference value only needs to be entered if the difference is greater than one minute. There is no need to synchronize differences of seconds less than one minute.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. When an error is detected, the monitor will immediately be scheduled to run again once.

Note: In order to change the run frequency of this monitor when an error is detected, you should use the **Error Frequency** option instead of the **Verify Error** option.

Note: The status returned by the **Verify Error** run of the monitor will replace the status of the originally scheduled run that detected an error. This may cause the loss of important performance data if the data from the verify run is different than the initial error status.

Use of this option across many monitor instances may result in significant monitoring delays in the case that multiple monitors are rescheduled to verify errors at the same time.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely

- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the status of this Remedy Ticketing monitor instance based on the results returned by the check.

Each Remedy Ticketing monitor instance has three status settings:

- **Error if**
- **Warning if**
- **Good if**

You can set unlimited threshold criteria for each status condition per Remedy Ticketing monitor instance. By default, only one threshold is displayed when you first configure the monitor.

While the monitor is enabled, it is assigned a status of good, warning, or error based on the most recent execution of the monitor action. The measurement taken or the results reported by the monitor are tested against the status threshold settings to determine the status.

The individual results are combined as logical **OR** relationships when more than one threshold condition is defined for any of the three settings. When one or more of the conditions (for example when two conditions for **Error if** setting) are met for a status setting the monitor status is set to the corresponding status condition. If status conditions are met for more than one status setting the status of the monitor is set to the highest valued status condition. For example, if one condition selected as Error if and another condition selected as Warning if are both met, the status would be reported as an error, with **error** being the highest value, **warning** the next highest and **good** the lowest value. The status is displayed by color and a status icon in the SiteScope interface.

A change of status signals an event and acts as a trigger for alerts associated with the monitor or the group to which the monitor belongs.

A change of status may also effect the state of a dependency between monitors. For example, a monitor that detects a change that results in a error status may be a trigger to disable one or more other monitors that are dependent on the Remedy Action Request System for ticket information.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement value. You may use the default status thresholds defined for the Remedy Ticketing or use the following steps to change the monitor status thresholds for this monitor instance:

To edit monitor status thresholds:

1. Use the first drop down menu to for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.

4 To add another threshold setting, click the **New Error If** button and repeat the steps above.

5 Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

115

Technology Database Integration Monitor

The Technology Database Integration Monitor allows you to collect event and time series data from database tables used by Enterprise Management Systems (EMS) by performing a query through a JDBC connection. The data retrieved is then processed and sent to Mercury Business Availability Center as samples (one sample for each row that was returned by an SQL query).

This chapter describes:	On page:
About the Technology Database Integration Monitor	1223
Setup Requirements	1225
Configuring the Technology Database Integration Monitor	1227
Step-by-Step Guide to Integrating Database Data into Mercury Business Availability Center	1237
Basic Troubleshooting	1240

About the Technology Database Integration Monitor

Use the Technology Database Integration Monitor in order to integrate database records into Mercury Business Availability Center. The following are examples of data that can be integrated into Mercury Business Availability Center using the Technology Database Integration Monitor:

- Events from monitoring applications event tables or views
- Open Tickets from ticketing systems applications
- Time series from monitoring applications measurement tables

---

Note: If you are upgrading SiteScope from version 7.8.1.2 or 7.9.0.0, see the note about upgrading Integration monitor types for version 7.9.1.0 or later in the section "Working with SiteScope Integration Monitors"

Each time the Technology Database Integration Monitor runs, it returns the monitors status, the time it took to perform the query, the number of rows in the query result set, and the first two fields in the first row of the result and writes them in the monitoring log file.

What Data Is Forwarded

The Technology Database Integration Monitor uses a user defined query and enumerating field name, field type, and initial value. While the query provided by the user is used to define a search criterion on the database, the enumerating field is used so that events are forwarded only once. Using an initial value allows you to specify an initial threshold value for the events that should be forwarded. For example, using `DATE` for the **Enumerating Field Type** with an **Start from value** of `2003-20-03 12:00:00` will forward only events that happened after the specified date in the first run of the monitor. In subsequent monitor runs the highest value for the DATE field found will be used to verify that only new events are forwarded.

You use the configuration file for the Technology Database Integration Monitor to control the data that is sent from SiteScope to Business Availability Center. See the section on "Integration Monitor Configuration Files" on page 1049 for more details on the file structure and syntax.

Before setting up the Technology Database Integration Monitor, you should be clear about the purpose and usage of the data in Mercury Business Availability Center (for presentation in Dashboard, Service Level Management, and/or reports).

Note: For information on Integration Monitor logging and troubleshooting, see Integration Monitor Logging Options and Troubleshooting Integration Monitors in Chapter 101, "Working with SiteScope Integration Monitors."

Setup Requirements

The steps for setting up a Technology Database Integration Monitor will vary according to what database software you are trying to query. The following is an overview of the requirements for using the Technology Database Integration Monitor:

- You must use one of the database drivers supplied by default, or install or copy a compatible database driver or database access API into the appropriate SiteScope directory location. The supplied drivers include:

  com.inet.tds.TdsDriver - (TDS driver from i-net Software for Microsoft SQL databases)

  com.inet.ora.OraDriver - (JDBC thin driver for Oracle databases)

  Many other database driver packages are available as compressed (zipped) archive files or .jar files. Database drivers in this form must NOT be extracted and must be installed into the <SiteScope root directory>\java\lib\ext subdirectory.

- You need to know the syntax for the Database Connection URL. The Database Connection URL normally includes the class of driver you are using, some key name relating to the supplier of the driver software, followed by a combination of server, host, and port identifiers. Examples of database connection URL's are:

  `jdbc:inetdae:`*`hostname`*`:`*`port`* - (where *`hostname`* is the name of the host where the database is running and *`port`* is the port on which the database interfaces with the driver)

  `jdbc:oracle:thin:@`*`hostname`*`:`*`port`*`:`*`dbname`* - (where *`hostname`* is the name of the host where the database is running, *`port`* is the port on

which the database interfaces with the driver, and *dbname* is the name of the Oracle database instance)

- The database you want to query must be running, have a database name defined, and have at least one named table created in the database. In some cases, the database management software needs to be configured to allow connections via the middleware or database driver.
- You need a valid username and password to access and perform a query on the database. In some cases, the machine and user account that SiteScope is running on must be given permissions to access the database.
- You need to know a valid SQL query string for the database instance and database table(s) in the database you want to extract data from. Consult your database administrator to work out appropriate queries to use.
- You need to create a configuration file for the Technology Database Integration Monitor and customize it for use with the specific system or application you will be monitoring. The configuration file controls what data is to be forwarded to Business Availability Center. The following steps outline the procedure for creating a configuration file for the Technology Database Integration Monitor.

  To create a configuration file:

1. On the server where SiteScope is running, open a sample configuration file with a text editor. Two sample template files are available: <SiteScope root directory>\conf\ems\templates\event.config and <SiteScope root directory>\conf\ems\templates\metrics.config.
2. Save a copy of the template configuration file into the <SiteScope root directory>\conf\ems\jdbc directory. You use this file to create your configuration file for the Technology Database Integration Monitor.
3. Edit the new file to define the event handlers for this monitor instance. See the section on "Integration Monitor Configuration Files" on page 1049 for more details on the file structure and syntax.

Note: When referring to data arriving from the Technology Database Integration Monitor in the config file, use the column name prefixed by the dollar sign ($).

For example, for the following database query:

SELECT height,width FROM some_table WHERE width > 0

You can refer to the columns returned using the labels: $height and $width

---

4 Save the changes to the configuration file. You enter the filename and path of this file relative to the SiteScope installation as the **EMS Configuration File Path** property when you set up the monitor.

Configuring the Technology Database Integration Monitor

The Technology Database Integration Monitor should be added to a SiteScope monitor group created for this monitor and other Integration Monitor types. It is recommended that you configure Integrations Monitors only after a connection between the SiteScope and Mercury Business Availability Center is established.

Note: SiteScope cannot be deployed behind a firewall. The SiteScope and the monitored system must be on the same LAN or special firewall configuration may be required.

Main Settings for the Technology Database Integration Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the target database, how often this Technology Database Integration Monitor instance should be run, and the text name used for this monitor instance in the interface. Complete the entries in the Main Settings section as described below. Complete the entries as needed and click the **OK** button to save the settings.

Name

Enter a text name for this Technology Database Integration monitor instance. This text is displayed in the Monitor Administration interface and in the SiteScope interface. If you do not enter a name text, a default name will be used.

Frequency

Select how often the Technology Database Integration monitor checks the database for data to forward to Mercury Business Availability Center. The default interval is to update once every 10 minutes. Use the drop-down list to the right of the text box to specify an update interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Database Connection URL

Enter a URL to a Database Connection (sometimes referred to as an Authentication string). One way to create a database connection is to use ODBC to create a named connection to a database. For example, first use the ODBC control panel to create a Data Source Name (DSN) called test under the system DSN tab. Then, enter jdbc:odbc:test in this box as the connection URL. Other way is to use the supplied MS SQL or Oracle driver in order to connect to the Database. When using the MS SQL driver, use the connection URL of the form jdbc:inetdae:<computer_name>:<port>?database=<db_name>. When using the Oracle driver, use the connection URL of the form jdbc:inetora:<computer_name>:<port>:<instance>.

Database Driver

Enter the driver used to connect to the database. Use the Fully Qualified Class Name of the JDBC driver you wish to use. The default drivers for this monitor are the com.inet.tds.TdsDriver - (TDS driver from i-net Software for Microsoft SQL databases) or oracle.jdbc.driver.OracleDriver - (JDBC thin driver for Oracle 7 and 8 databases). When using OBBC-JDBC connection, you may use sun.jdbc.odbc.JdbcOdbcDriver.

SELECT

Enter the SELECT clause to be used in the SQL query. Enter * for all fields or a comma separated list of column names to be retrieved from the database.

Note: When specifying the **SELECT** clause, the column used as the enumerating field must appear in the clause.

FROM

Enter the FROM clause to be used in the SQL query. Enter a table name or a comma separated list of tables from which the selected columns should be extracted.

WHERE

Enter the WHERE clause to be used in the SQL query. This is an optional field which allows you to define the select criteria. Leaving it empty will result in retrieving all the rows from the table defined in the FROM option.

Database Username

Enter the username used to login to the database.

Database Password

Enter a password used to login to the database.

Enumerating Field

Enter a name for a database field that can be used to order the events that are returned from the database query.

Note: The column used as enumerating field must be included in the **SELECT** clause.

Enumerating Field Type

Enter the type of field used to order the result set. This can be a DATE field, an INTEGER field or a DOUBLE floating point numeral field.

The following table maps SQL types to the appropriate enumerating field type.

SQL Type	Enumerating Field Type
SMALLINT	INTEGER
INTEGER	INTEGER / LONG
BIGINT	LONG
NUMERIC	LONG
DOUBLE	DOUBLE
DECIMAL	DOUBLE
FLOAT	DOUBLE
TIMESTAMP	TIMESTAMP
DATE	TIMESTAMP

Note: Some SQL types can work with more then one enumerating field type. It is recommended to use the mapping above in order to ensure accurate results.

When working with an SQL server, the SQL Integer type can be either INTEGER or LONG.

Initial Enumerating Value

Enter an initial value that will be used as a condition for the initial run of this monitor instance. If for example, you specify the Enumerating Field Type as a field type DATE and you enter a value of 2000-31-01 12:00:00 in the Start from value field, only records which were added to the database after the specified date will be forwarded.

The value of this field cannot be edited.

EMS Configuration File Path

Enter the path to the EMS integration configuration file that you create for this monitor. See the procedure for creating the file in the section "Setup Requirements" on page 1225. For more information about the format of the file see the section on "Integration Monitor Configuration Files" on page 1049. You can store the file in the: <SiteScope root directory>\conf\ems\JDBC directory.

Advanced Settings for the Technology Database Integration Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Technology Database Integration Monitor and its display in the product interface. Use this section to set monitor-to-monitor dependencies, customize display options, and configure other settings specific to the Technology Database Integration Monitor that may be required in some infrastructure environments. Complete the entries as needed and click the **OK** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Maximum Number of Rows to Retrieve

Specify the maximum number of rows the monitor retrieves from the database for each monitor cycle. The default value is 5000.

If the number of result rows exceeds the set maximum, the monitor will retrieve the remaining rows (those that exceeded the maximum) on future cycles, until all result rows are retrieved.

The Max Rows value should be large enough to keep up with database table growth, yet small enough to avoid java.lang.OutOfMemoryException errors. Further, monitor run frequency should also be considered. Make sure that the rate at which data is collected by the monitor—which is dependent upon both monitor run frequency and network/system speed—is greater than or equal to the rate of data insertion on the monitored system.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. You may, however, schedule your monitors to run only on certain days or on a fixed schedule. Click the Edit schedule link to create or edit a monitor schedule. For more information about working with monitor schedules, see the section on Schedule Preferences for Monitoring.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the other monitor should have for the current monitor to run normally. The current monitor will be run normally as long as the monitor selected in the **Depends On** field reports the condition selected in this field. For example, by selecting OK, this monitor is only enabled as long as the monitor selected in the **Depends On** field reports a status of good or OK.

Monitor Description

Enter additional information to describe this monitor. The Monitor Description can include HTML tags such as the <BR>, <HR>, and <B> tags to control display format and style. The description text will appear on the Monitor Detail page.

Report Description

Enter an optional description for this monitor that will make it easier to understand what the monitor does. For example, network traffic or main server response time. This description will be displayed on with each bar chart and graph in Management Reports and appended to the tool-tip displayed when you pass the mouse cursor over the status icon for this monitor on the Monitor Detail page.

EMS Time Difference

Use this option to account for time differences between the system clock time on the monitored EMS machine and the server where SiteScope is running. This is only needed when the EMS data includes time data and the time data shows that there is a time difference between the EMS machine and the SiteScope server. If the time difference is too great the data may be discarded from Mercury Business Availability Center.

Note: The time difference value only needs to be entered if the difference is greater than one minute. There is no need to synchronize differences of seconds less than one minute.

DB Machine Name

If you are reporting monitor data to an installation of Mercury Business Availability Center, enter a text identifier describing the database server that this monitor is monitoring. This text descriptor is used to identify the database server when the monitor data is viewed in a Mercury Business Availability Center report. Use only alphanumeric characters for this entry. You can enter the name of the monitored server or a description of the database that will be used to identify the host.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. When an error is detected, the monitor will immediately be scheduled to run again once.

Note: In order to change the run frequency of this monitor when an error is detected, you should use the **Error Frequency** option instead of the **Verify Error** option.

Note: The status returned by the **Verify Error** run of the monitor will replace the status of the originally scheduled run that detected an error. This may cause the loss of important performance data if the data from the verify run is different than the initial error status.

Use of this option across many monitor instances may result in significant monitoring delays in the case that multiple monitors are rescheduled to verify errors at the same time.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the status settings to set threshold conditions that determine the status of this Technology Database Integration monitor instance based on the results returned by the check.

Each Technology Database Integration monitor instance has three status settings:

- **Error if**
- **Warning if**
- **Good if**

While the monitor is enabled, it is assigned a status of good, warning, or error based on the most recent execution of the monitor action. The measurement taken or the results reported by the monitor are tested against the status threshold settings to determine the status. The status is displayed by color and a status icon in the SiteScope interface.

A change of status acts as a trigger for alerts associated with the monitor or the group to which the monitor belongs. For example, if the Technology Database Integration Monitor detects that the target database has become unavailable, the status change from good to error is used to trigger an alert on error.

A change of status may also effect the state of a dependency between monitors.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement value. You may use the default status thresholds defined for the Technology Database Integration or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop down menu to for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. Repeat these steps for the Warning if and Good if settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

Step-by-Step Guide to Integrating Database Data into Mercury Business Availability Center

This section provides the overall flow for setting up the Technology Database Integration Monitor to work with Mercury Business Availability Center 5.1. If you need more information on performing any of the steps, see the sections on "Setup Requirements" on page 1225, and "Configuring the Technology Database Integration Monitor" on page 1227.

To integrate database data into Mercury Business Availability Center:

1 Use a database client to connect to the relevant software database. Identify which tables contain the required events/metrics (the software schema documentation may help you with this).

2 A JDBC database driver is a prerequisite for setting up the monitor. It is recommended to use the following JDBC drivers:

- For SQL Server:

  Database Connection URL=
  jdbc:inetdae:<DatabaseHostName>:<Port>?database=<Database Name>

  Database Driver=com.inet.tds.TdsDriver

- For Oracle:

  Database Connection URL=
  jdbc:inetora:<DatabaseHostName>:<Port>:<Database Instance Name>

  Database Driver=com.inet.ora.OraDriver

3 Use the Sitescope Database Connection tool as follows:

- Verify the driver can be loaded and that it successfully connects.
- Add a username and password to verify that a connection can be established to the database.
- Add a naive query. Refine the query until you get all the required events/metrics required for usage in Mercury Business Availability Center.

4 Save a copy of one of the templates from <SiteScope root directory>\conf\ems\templates to the <SiteScope root directory>\conf\ems\jdbc directory. For events integration, use the **event.config** template, or for metrics integration, use the **metrics.config** template. It is recommended that you change the name of the .config file copy to include the name of the integrated software, for example: avalon.config.

5 Edit the saved .config file according to the data that you want to see in Mercury Business Availability Center. Refer to columns by their database name, prefixed with the **$** character. Field name with space(s) should be enclosed in square brackets **[ ]** in the query—however, it is recommended to select using the **as** option. (If you use **as**, then refer to the **as** attribute in the .config file.)

See the section on "Integration Monitor Configuration Files" on page 1049 for more details on the file structure and syntax.

6 Verify that your .config file syntax is correct by running <SiteScope root directory>\conf\ems\tools\test_config.bat <full path to your saved .config file> on the SiteScope machine.

7 Add a Technology Database Integration Monitor in Mercury Business Availability Center Monitor Administration, as described in "Configuring the Technology Database Integration Monitor" on page 1227. Note the following:

- When adding the new monitor to a group, it is recommended that you use a dedicated group for integration monitors only.
- You add the **Technology Database Integration Monitor** from the **Integration Monitors** section in the New SiteScope Monitor pane. If you do not see the **Integration Monitors** section, make sure you have an EMS Option License for your SiteScope.

8 In the New Monitor pane for the Technology Database Integration Monitor, make sure that a value is specified for all parameters in the **Main Settings** section.

Note the following:

- **Name** – It is recommended that the monitor name include the name of the integrated software.
- **Connection parameters** – Fill all connection parameters for connecting to the database: **Database Connection URL**; **Database User Name**; **Database Password**; **Database Driver**
- **SELECT/FROM/WHERE** query clauses – **SELECT** and **FROM** are mandatory. It is recommended that you build your query with the SiteScope Database Connection tool *before* defining the monitor. When specifying the **SELECT** clause, the value given for **Enumerating Field** must appear in the clause.
- **Frequency** – Define how often the monitor should query the database. For SiteScope 7.9.5, the maximum number of rows that the monitor can retrieve on each cycle is 5000; this is to prevent an out-of-memory exception. The frequency should therefore be set so that the monitor retrieves a maximum of 5000 rows per cycle.

  For SiteScope 8.x, you can edit the maximum number of rows in the **Advanced Settings** section for the monitor.
- **Enumerating Field parameters** – Fill in details for the enumerating field.
- **EMS Configuration File Path** – Enter the full path of the .config file on the SiteScope machine (for example: D:\<SiteScope root directory>\conf\ems\jdbc\myconfig.config).

9 View the data in Mercury Business Availability Center:

- **Events integration** – you can view events in Dashboard (add a Generic EMS source, then add the Generic EMS NodeFactory to a view), System Availability Management Event Log reports, or Analytics. You can also use events when building SLAs.
- **Metrics integration** – you can view the data in any application that supports SiteScope data, including SiteScope reports.

➤ If you want to watch the incoming samples (to view the original data before it is passed to the applications), use the sprinter utility available under <Mercury Business Availability Center root directory>\bin.

To troubleshoot problems with data arriving to Mercury Business Availability Center, see "Basic Troubleshooting" on page 1240.

Basic Troubleshooting

➤ Check for errors in <SiteScope root directory>\logs\EmsMonitors.log and in <SiteScope root directory>\logs\error.log.

➤ Change the log level to DEBUG in <SiteScope root directory>\conf\log4j.properties, in order to watch outgoing samples.

Change the line:
log4j.category.EmsEventPrinter=${emsloglevel}, ems.appender
to:
log4j.category.EmsEventPrinter= DEBUG, ems.appender.

The log file to look at is:
<SiteScope root directory>\logs\EmsMonitors.log

➤ If samples are created and sent from SiteScope, but the data is not seen in Dashboard/Event Log/SiteScope reports: Look in <Mercury Business Availability Center root directory>\log\dispatcher_log.txt to make sure the samples were not dropped due to missing fields or values.

➤ Use <Mercury Business Availability Center root directory>\bin\sprinter.exe to view sample flow on the bus. Run the executable without parameters in order to get help.

➤ Change the logging level for Dashboard to verify that Dashboard received the samples. Open:
<Mercury Business Availability Center root directory>\conf\log4j4EJB.properties

Change the log level parameter to DEBUG in the following line:
log4j.category.JMDRVSamples=DEBUG,jmdrv.samples.appender

The log file to look at is:
<Mercury Business Availability Center root directory>\log\
EJBContainer\TrinitySamples.log

116

Technology Log File Integration Monitor

The Technology Log File Integration Monitor watches for specific entries added to a log file of a Enterprise Management System (EMS) application by trying to match against a regular expression. From each matched entry one sample is created and sent to Mercury Business Availability Center. Each time the monitor runs, it examines log entries added since the last time it ran.

This chapter describes:	On page:
About the Technology Log File Integration Monitor	1243
Setup Requirements	1244
Configuring the Technology Log File Integration Monitor	1246
Step-by-Step Guide to Integrating Log File Data into Mercury Business Availability Center	1256
Basic Troubleshooting	1259

About the Technology Log File Integration Monitor

The Technology Log File Integration Monitor is useful for automatically extracting data from log files and sending the data to Mercury Business Availability Center. For example, you can use this monitor to forward information from Hewlett Packard Network Node Manager to Business Availability Center.

Each time that it runs this monitor, SiteScope starts from the point in the file where it stopped reading the last time it ran. This insures that you are notified only of new entries and speeds the rate at which the monitor runs.

When using a regular expression to match against a specific line in the log, it is possible to use regular expression back references to select the data to be forwarded to Business Availability Center. See "Retaining Content Match Values" in *Advanced Monitor Options* for more details on using back references.

Note: If you are upgrading SiteScope from version 7.8.1.2 or 7.9.0.0, see the note about upgrading Integration monitor types for version 7.9.1.0 or later in the section "Working with SiteScope Integration Monitors"

What Data Is Collected

The EMS Log File monitor sends to Business Availability Center data that is extracted from any row that matched against the **Content Match** regular expression.

Before setting up the Technology Log File Integration Monitor, you should be clear about the purpose and usage of the data in Mercury Business Availability Center (for presentation in Dashboard, Service Level Management, and/or reports).

Note: For information on Integration Monitor logging and troubleshooting, see Integration Monitor Logging Options and Troubleshooting Integration Monitors in Chapter 101, "Working with SiteScope Integration Monitors."

Setup Requirements

The following are requirements for using the Technology Log File Integration Monitor to forward data to Business Availability Center:

- You need to know the format and syntax of the log file that you want to monitor. You will need to construct a **Content Match** regular expression to match on the entries in the log file that contain the data you want to monitor and forward to Business Availability Center. For example regular expressions, see "Examples for Log File Monitoring" in *Advanced Monitor Options*.
- You need to create a configuration file for the Technology Log File Integration Monitor and customize it for use with the specific system or application you will be monitoring. The configuration file controls what data is to be forwarded to Business Availability Center. The following steps outline the procedure for creating a configuration file for the Technology Log File Integration Monitor.

To create a configuration file:

1. On the server where SiteScope is running, open a sample configuration file with a text editor. Two sample template files are available: <SiteScope root directory>/conf/ems/templates/event.config and <SiteScope root directory>/conf/ems/templates/metrics.config.
2. Save a copy of the template configuration file into the <SiteScope root directory>/conf/ems/logfile directory. You use this file to create your configuration file for the Technology Log File Integration Monitor.
3. Edit the new file to define the event handlers for this monitor instance. See the section on "Integration Monitor Configuration Files" on page 1049 for more details on the file structure and syntax.

Note: When referring to data arriving from the Technology Log File Integration monitor in the configuration file, use the number corresponding to the back reference returned prefixed by the label $group

For example, for the **Content Match** expression:

/([0-9]{2})\s([A-Z]*) ([a-z]*) /

and the corresponding Log file text that contains:

21 HELLO world

You can refer in the config file to three retained values (back references) as follows, where the number appended to the end of the $groupn label corresponds to the order of the parentheses in the expression:

$group0 = (21)
$group1 = (HELLO)
$group2 = (world)

---

4 Save the changes to the configuration file. You enter the filename and path of this file relative to the SiteScope installation as the **EMS Configuration File Path** property when you set up the monitor.

Configuring the Technology Log File Integration Monitor

The Technology Log File Integration Monitor should be added to a SiteScope monitor group created for this monitor and other Integration Monitor types. It is recommended that you configure Integrations Monitors only after a connection between the SiteScope and Mercury Business Availability Center is established.

Note: SiteScope cannot be deployed behind a firewall. The SiteScope and the monitored system must be on the same LAN or special firewall configuration may be required.

Main Settings for the Technology Log File Integration Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the target log file, how often this Technology Log File Integration Monitor instance should be run, and the text name used for this monitor instance in the interface. Complete the entries in the Main Settings section as described below. Complete the entries as needed and click the **OK** button to save the settings.

Name

Enter a text name for this Technology Log File Integration monitor instance. This text is displayed in the Monitor Administration interface and in the SiteScope interface. If you do not enter a name text, a default name will be used.

Frequency

Select how often the Technology Log File Integration monitor checks the log file for data to forward to Mercury Business Availability Center. The default interval is to update once every 10 minutes. Use the drop-down list to the right of the text box to specify an update interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Servers

Choose the server where the log file you want to monitor is located. Use the drop-down list to select a server from the list of UNIX remote servers that are available to the SiteScope agent.

Log File Pathname

Enter the pathname to the log file you want to extract data from. For reading log files on remote UNIX machines, the path must be relative to the home directory of UNIX user account being used to login to the remote machine. See the **Preferences > UNIX Servers** page for information on which UNIX user account is being used.

You can also monitor log files on a remote Windows NT/2000 server through NetBIOS by including the UNC path to the remote log file. For example,

\\remoteserver\sharedfolder\filename.log

This requires that the user account under which SiteScope is running has permission to access the remote directory using the UNC path. If a direct connection via the operating system is unsuccessful, SiteScope will try to match the `\\remoteserver` with servers currently defined as remote NT connection profiles (displayed in the Remote NT Servers table). If an exact match is found for `\\remoteserver` in the remote NT connection profiles, SiteScope will try to use this connection profile to access the remote log file. If no matching server name is found, the monitor reports that the remote log file can not be found.

Note: If you are using SSH as a connection method to remote NT servers, you will need to select the remote server using the **Server** selection above. It is not necessary to select a remote NT server if you are using NetBIOS to connect to remote NT servers.

Optionally, you can use a regular expression to insert date and time variables. For example, you can use a syntax of

s/ex$shortYear$$0month$$0day$.log/

to match date-coded IIS log file names.

Log File Encoding

If you are reading a log file whose encoding is different than the SiteScope machine's default encoding, specify the log file encoding.

Content Match

Enter the text to look for in the log entries. You can also use regular expression in this entry to match text patterns. Unlike the content match feature of other SiteScope monitors, the Log File Monitor content match is run repeatedly against the most recent content of target log file until all matches are found. This means the monitor not only reports if the match was found but also how many times the matched pattern was found. To match text that includes more than one line of text, add an s search modifier to the end of the regular expression.

EMS Configuration File Path

Enter the path to the EMS integration configuration file relative to the SiteScope installation that you create for this monitor. See the procedure for creating the file in the section "Setup Requirements" on page 1244. For more information about the format of the file, see the section on "Integration Monitor Configuration Files" on page 1049. Templates for creating configuration file are available in: <SiteScope root directory>\conf\ems\templates. You can store the file in the: <SiteScope root directory>\conf\ems\logfile directory.

Advanced Settings for the Technology Log File Integration Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Technology Log File Integration Monitor and its display in the product interface. Use this section to set monitor-to-monitor dependencies, customize display options, and configure other settings specific to the Technology Log File Integration Monitor that may be required in some infrastructure environments. Complete the entries as needed and click the **OK** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

No Error if File Not Found

Check this box if you want this monitor to remain in GOOD status, if the file is not found.

Run Alerts

Select the method for running alerts for this monitor.

- Select "**for each log entry matched**" to have the monitor trigger alerts for each and every matching entry found.
  Note: When the Technology Log File Integration Monitor is run with this alert method selected, the monitor will never be displayed as an error or warning status in the SiteScope interface, regardless of the results of the content match or even if the target log file is not found. The monitor will trigger alerts if one or more matching entries are found and the **Error if** or **Warning if** thresholds are defined accordingly in the Advanced Options section. For example, setting **Error if** to the default of `matchCount > 0`.
- Select "**once, after all log entries have been checked**" to have the monitor count up the number of matches and trigger alerts one time based on the **Error if** and **Warning if** thresholds defined for the monitor in the Advanced Options section.

Note: By default, selecting this option will cause SiteScope to send one alert message if one or more matches are found, but the alert will not include any details of the matching entries. To have SiteScope include the matching entries, you must associate the monitor with an alert definition that has the property, <matchDetails> in the alert template. This special template property is used to populate the alert with the details of all the matching entries. You use this for e-mail alerts or other alert types that work with template properties. E-mail alert templates are stored in the SiteScope\templates.mail directory. See the chapter on Custom Alert Templates in the SiteScope Reference Guide for more information about modifying alert templates.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. You may, however, schedule your monitors to run only on certain days or on a fixed schedule. Click the Edit schedule link to create or edit a monitor schedule. For more information about working with monitor schedules, see the section on Schedule Preferences for Monitoring.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the other monitor should have for the current monitor to run normally. The current monitor will be run normally as long as the monitor selected in the **Depends On** field reports the condition selected in this field. For example, by selecting OK, this monitor is only enabled as long as the monitor selected in the **Depends On** field reports a status of good or OK.

Monitor Description

Enter additional information to describe this monitor. The Monitor Description can include HTML tags such as the <BR>, <HR>, and <B> tags to control display format and style. The description text will appear on the Monitor Detail page.

Report Description

Enter an optional description for this monitor that will make it easier to understand what the monitor does. For example, network traffic or main server response time. This description will be displayed on with each bar chart and graph in Management Reports and appended to the tool-tip displayed when you pass the mouse cursor over the status icon for this monitor on the Monitor Detail page.

EMS Time Difference

Use this option to account for time differences between the system clock time on the monitored EMS machine and the server where SiteScope is running. This is only needed when the EMS data includes time data and the time data shows that there is a time difference between the EMS machine and the SiteScope server. If the time difference is too great the data may be discarded from Mercury Business Availability Center.

Note: The time difference value only needs to be entered if the difference is greater than one minute. There is no need to synchronize differences of seconds less than one minute.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. When an error is detected, the monitor will immediately be scheduled to run again once.

Note: In order to change the run frequency of this monitor when an error is detected, you should use the **Error Frequency** option instead of the **Verify Error** option.

Note: The status returned by the **Verify Error** run of the monitor will replace the status of the originally scheduled run that detected an error. This may cause the loss of important performance data if the data from the verify run is different than the initial error status.

Use of this option across many monitor instances may result in significant monitoring delays in the case that multiple monitors are rescheduled to verify errors at the same time.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the status of this Technology Log File Integration monitor instance based on the results returned by the check.

Each Technology Log File Integration monitor instance has three status settings:

- **Error if**
- **Warning if**
- **Good if**

You can set unlimited threshold criteria for each status condition per Technology Log File Integration monitor instance. By default, only one threshold is displayed when you first configure the monitor.

While the monitor is enabled, it is assigned a status of good, warning, or error based on the most recent execution of the monitor action. The measurement taken or the results reported by the monitor are tested against the status threshold settings to determine the status.

The individual results are combined as logical **OR** relationships when more than one threshold condition is defined for any of the three settings. When one or more of the conditions (for example when two conditions for **Error if** setting) are met for a status setting the monitor status is set to the corresponding status condition. If status conditions are met for more than one status setting the status of the monitor is set to the highest valued status condition. For example, if one condition selected as Error if and another condition selected as Warning if are both met, the status would be reported as an error, with **error** being the highest value, **warning** the next highest and **good** the lowest value. The status is displayed by color and a status icon in the SiteScope interface.

A change of status signals an event and acts as a trigger for alerts associated with the monitor or the group to which the monitor belongs.

A change of status may also effect the state of a dependency between monitors. For example, a monitor that detects a change that results in a error status may be a trigger to disable one or more other monitors that are dependent on the target log file.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement value. You may use the default status thresholds defined for the Technology Log File Integration or use the following steps to change the monitor status thresholds for this monitor instance:

To edit monitor status thresholds:

1. Use the first drop down menu to for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.

5 Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

Step-by-Step Guide to Integrating Log File Data into Mercury Business Availability Center

This section provides the overall flow for setting up the Technology Log File Integration Monitor to work with Mercury Business Availability Center 5.1. If you need more information on performing any of the steps, see the sections on "Setup Requirements" on page 1244, or "Configuring the Technology Log File Integration Monitor" on page 1246.

To integrate log file data into Mercury Business Availability Center:

1 Open the relevant software log file, and identify which lines describe events or metrics. Build your regular expression with the SiteScope Regular Expression tool. Use the tool to:

➤ match against the line you wish to use.

➤ make sure that values extracted correctly from the line.

2 Save a copy of one of the templates from <SiteScope root directory>\conf\ems\templates to the <SiteScope root directory>\conf\ems\logfile directory. For events integration, use the **event.config** template, or for metrics integration, use the **metrics.config** template. It is recommended that you change the name of the .config file copy to include the name of the integrated software, for example: avalon.config.

3 Edit the saved .config file according to the data that you want to see in Mercury Business Availability Center. Refer to extracted values by **group*** prefixed with the **$** character, starting from **$group0**. See the section on "Integration Monitor Configuration Files" on page 1049 for more details on the file structure and syntax.

4 Verify that your .config file syntax is correct by running <SiteScope root directory>\conf\ems\tools\test_config.bat <full path to your saved .config file> on the SiteScope machine.

5 Add a Technology Log File Integration Monitor in Mercury Business Availability Center Monitor Administration, as described in "Configuring the Technology Log File Integration Monitor" on page 1246. Note the following:

➤ When adding the new monitor to a group, it is recommended that you use a dedicated group for integration monitors only.

➤ You add the **Technology Log File Integration Monitor** from the **Integration Monitors** section in the New SiteScope Monitor pane. If you do not see the **Integration Monitors** section, make sure you have an EMS Option License for your SiteScope.

6 In the New Monitor pane for the Technology Log File Integration Monitor, make sure that a value is specified for all parameters in the **Main Settings** section.

Note the following:

➤ **Name** – It is recommended that the monitor name include the name of the integrated software.

➤ **Log File Pathname** and **Server**:

- The file name can include a variable name (for example: **s/c:\temp\EV-$year$-$0month$-$0day$.tab/**).
- When reading a file on a remote UNIX machine, define a remote UNIX connection; you can then select the UNIX machine from the **Server** list.
- When reading a file on a remote Windows machine, enter the UNC path in the **Log File Pathname** box (SiteScope should run under a privileged user for the machine that holds the file), and leave the **Server** box empty.

➤ **Frequency** – Specify how often the monitor should query the log file.

➤ **Content Match** (regular expression) – Surround values you wish to extract with parenthesis. It is recommended that you build your content match with the SiteScope Regular Expression tool before defining the monitor.

➤ **EMS Configuration File Path** – Enter the full path of the .config file on the SiteScope machine (for example: D:\<SiteScope root directory>\conf\ems\logfile\myconfig.config).

7 It is recommended that you perform optimization of the regular expression after completing setup of the Technology Log File Integration Monitor (for example, to check for problems with use of quantifiers such as **.***). Optimization is done with the SiteScope Regular Expression tool. Update the monitor with any corrections.

8 View the data in Mercury Business Availability Center:

➤ **Events integration** – you can view events in Dashboard (add a Generic EMS source, then add the Generic EMS NodeFactory to a view), System Availability Management Event Log reports, or Analytics. You can also use events when building SLAs.

➤ **Metrics integration** – you can view the data in any application that supports SiteScope data, including SiteScope reports.

➤ If you want to watch the incoming samples (to view the original data before it is passed to the applications), use the sprinter utility available under <Mercury Business Availability Center root directory>\bin.

To troubleshoot problems with data arriving to Mercury Business Availability Center, see "Basic Troubleshooting" on page 1259.

Basic Troubleshooting

- Check for errors in <SiteScope root directory>\logs\EmsMonitors.log and in <SiteScope root directory>\logs\error.log.
- Change the log level to DEBUG in <SiteScope root directory>\conf\log4j.properties, in order to watch outgoing samples.

  Change the line:
  log4j.category.EmsEventPrinter=${emsloglevel}, ems.appender
  to:
  log4j.category.EmsEventPrinter= DEBUG, ems.appender.

  The log file to look at is:
  <SiteScope root directory>\logs\EmsMonitors.log
- If samples are created and sent from SiteScope, but the data is not seen in Dashboard/Event Log/SiteScope reports: Look in <Mercury Business Availability Center root directory>\log\dispatcher_log.txt to make sure the samples were not dropped due to missing fields or values.
- Use <Mercury Business Availability Center root directory>\bin\sprinter.exe to view sample flow on the bus. Run the executable without parameters in order to get help.
- Change the logging level for Dashboard to verify that Dashboard received the samples. Open:
  <Mercury Business Availability Center root directory>\conf\
  log4j4EJB.properties

  Change the log level parameter to DEBUG in the following line:
  log4j.category.JMDRVSamples=DEBUG,jmdrv.samples.appender

  The log file to look at is:
  <Mercury Business Availability Center root directory>\log\
  EJBContainer\TrinitySamples.log

117

Technology SNMP Trap Integration Monitor

The Technology SNMP Trap Integration Monitor watches for SNMP traps received by SiteScope from third-party Enterprise Management Systems (EMS). For each SNMP trap that SiteScope receives, a sample is forwarded to Mercury Business Availability Center containing the SNMP trap values.

The third-party EMS systems need to be configured to send traps to the SiteScope server.

This chapter describes:	On page:
About the Technology SNMP Trap Integration Monitor	1261
Setup Requirements	1262
Configuring the Technology SNMP Trap Integration Monitor	1264
Step-by-Step Guide to Integrating SNMP Trap Data into Mercury Business Availability Center	1272
Troubleshooting the Technology SNMP Trap Integration Monitor	1274

About the Technology SNMP Trap Integration Monitor

The Technology SNMP Trap Integration Monitor is useful for integrating traps that your external devices generate into the Mercury Business Availability Center framework. For example, you can use this monitor to forward information from Hewlett Packard Network Node Manager to Business Availability Center. See “Integration with HP Network Node Manager” on page 1325 for more information.

Note: For information on Integration Monitor logging and troubleshooting, see Integration Monitor Logging Options and Troubleshooting Integration Monitors in Chapter 101, "Working with SiteScope Integration Monitors."

Note: If you are upgrading SiteScope from version 7.8.1.2 or 7.9.0.0, see the note about upgrading Integration Monitor types for version 7.9.1.0 or later in the section "Working with SiteScope Integration Monitors"

What Data Is Being Collected?

The Technology SNMP Trap Integration Monitor collects data that is extracted from any SNMP trap received by SiteScope and sends notifications to Mercury Business Availability Center containing preferred values from the original SNMP trap.

Before setting up the Technology SNMP Trap Integration Monitor, you should be clear about the purpose and usage of the data in Mercury Business Availability Center (for presentation in Dashboard, Service Level Management, and/or reports).

The specific data that is forward to Mercury Business Availability Center is controlled by a configuration file for the Technology SNMP Trap Integration Monitor. You use this file to specify the preferred value fields that you want forwarded. A sample template file is provided in the <SiteScope root directory>\conf\ems\templates\event.config. See the section on "Integration Monitor Configuration Files" on page 1049 for more details on the file structure and syntax.

Setup Requirements

The following are requirements for using the Technology SNMP Trap Integration Monitor to forward data to Business Availability Center:

- SiteScope must be registered with a Business Availability Center installation. The SiteScope must have a profile defined in the Business Availability Center installation prior to enabling the registration in the SiteScope interface. In order to verify registration or to re-register SiteScope with the Business Availability Center server, see the Mercury Business Availability Center Server Registration page under SiteScope Preferences.
- You need to create a configuration file for the Technology SNMP Trap Integration Monitor and customize it for use with the specific system or application you will be monitoring. The configuration file controls what data is to be forwarded to Business Availability Center. The following steps outline the procedure for creating a configuration file for the Technology SNMP Trap Integration Monitor.

To create a configuration file:

1. On the server where SiteScope is running, open a sample configuration file with a text editor. A sample template file is available: <SiteScope root directory>\conf\ems\templates\event.config.
2. Save a copy of the template configuration file into the <SiteScope root directory>\conf\ems\snmptrap directory. You use this file to create your configuration file for the Technology SNMP Trap Integration Monitor.
3. Edit the new file to define the event handlers for this monitor instance. See the section on "Integration Monitor Configuration Files" on page 1049 for more details on the file structure and syntax.

Note: All the received traps will be saved to **snmptrap.log** in <**SiteScope root directory**>**logs**. When referring to data arriving from the Technology SNMP Trap Integration Monitor in the config file, use the names from the snmptrap.log file, prefixed with the dollar sign ($). For example:

Use the $oid fto refer to the oid value of the trap, $var1 to refer to the variable bound as the first variable in trap, and $var2 for variable bound as second variable in trap.

---

4. Save the changes to the configuration file. You enter the filename and path of this file relative to the SiteScope installation as the **EMS Configuration File Path** property when you set up the monitor.

➤ The SNMP agents you want to monitor must be configured to send SNMP traps to the SiteScope host. Consult with the system administrator or applicable product documentation for more information on SNMP configuration.

Note: The Technology SNMP Trap Integration Monitor uses port 162 for receiving traps. If another application or process on the machine where SiteScope is running has bound this port, the monitor will report an "Address in use" error and the monitor type will be unavailable. You will have to terminate the process or service that is using the port, and restart SiteScope afterwards.

Configuring the Technology SNMP Trap Integration Monitor

The Technology SNMP Trap Integration Monitor should be added to a SiteScope monitor group created for this monitor and other Integration Monitor types. It is recommended that you configure Integrations Monitors only after a connection between the SiteScope and Mercury Business Availability Center is established.

Note: SiteScope cannot be deployed behind a firewall. The SiteScope and the monitored system must be on the same LAN or special firewall configuration may be required.

Main Settings for the Technology SNMP Trap Integration Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the SNMP trap data and the text name used for this monitor instance in the interface. Complete the entries in the Main Settings section as described below. Complete the entries as needed and click the **OK** button to save the settings.

Name

Enter a text name for this Technology SNMP Trap Integration monitor instance. This text is displayed in the Monitor Administration interface and in the SiteScope interface. If you do not enter a name text, a default name will be used.

EMS Configuration File Path

Enter the path to the EMS integration configuration file relative to the SiteScope installation that you create for this monitor. See the procedure for creating the file in the section "Setup Requirements" on page 1262. For more information about the format of the file see the section on "Integration Monitor Configuration Files" on page 1049 for details on the configuration file format. You can store the file in the: <SiteScope root directory>\conf\ems\snmptrap directory.

Advanced Settings for the Technology SNMP Trap Integration Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Technology SNMP Trap Integration Monitor and its display in the product interface. Use this section to set monitor-to-monitor dependencies, customize display options, and configure other settings specific to the Technology SNMP Trap Integration Monitor that may be required in some infrastructure environments. Complete the entries as needed and click the **OK** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Frequency

Select how often the monitor should update its status. The **Frequency** setting for the Technology SNMP Trap Integration Monitor controls only the status reports. The SNMP trap data are forwarded when they are received without any delay. The default interval is to update once every 10 minutes. Use the drop-down list to the right of the text box to specify an update interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Run Alerts

Choose the method for running alerts. If for each SNMP Trap received from EMS system is chosen, then the monitor triggers alerts for every matching entry found.

Note: When the Technology SNMP Trap Integration Monitor is run in the for each SNMP Trap received from EMS system alert method, the monitor will never report a status of error or warning, regardless of the results of the content match or even if the target SNMP Trap is not found.

If the once, after all SNMP Traps from EMS system were received method is chosen, then the monitor counts up the number of matches and triggers alerts based on the "Error If" and "Warning If" thresholds defined for the monitor in the Advanced Settings section.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. You may, however, schedule your monitors to run only on certain days or on a fixed schedule. Click the Edit schedule link to create or edit a monitor schedule. For more information about working with monitor schedules, see the section on Schedule Preferences for Monitoring.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the other monitor should have for the current monitor to run normally. The current monitor will be run normally as long as the monitor selected in the **Depends On** field reports the condition selected in this field. For example, by selecting OK, this monitor is only enabled as long as the monitor selected in the **Depends On** field reports a status of good or OK.

Monitor Description

Enter additional information to describe this monitor. The Monitor Description can include HTML tags such as the <BR>, <HR>, and <B> tags to control display format and style. The description text will appear on the Monitor Detail page.

Report Description

Enter an optional description for this monitor that will make it easier to understand what the monitor does. For example, network traffic or main server response time. This description will be displayed on with each bar chart and graph in Management Reports and appended to the tool-tip displayed when you pass the mouse cursor over the status icon for this monitor on the Monitor Detail page.

EMS Time Difference

Use this option to account for time differences between the system clock time on the monitored EMS machine and the server where SiteScope is running. This is only needed when the EMS data includes time data and the time data shows that there is a time difference between the EMS machine and the SiteScope server. If the time difference is too great the data may be discarded from Mercury Business Availability Center.

Note: The time difference value only needs to be entered if the difference is greater than one minute. There is no need to synchronize differences of seconds less than one minute.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. When an error is detected, the monitor will immediately be scheduled to run again once.

Note: In order to change the run frequency of this monitor when an error is detected, you should use the **Error Frequency** option instead of the **Verify Error** option.

Note: The status returned by the **Verify Error** run of the monitor will replace the status of the originally scheduled run that detected an error. This may cause the loss of important performance data if the data from the verify run is different than the initial error status.

Use of this option across many monitor instances may result in significant monitoring delays in the case that multiple monitors are rescheduled to verify errors at the same time.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the status of this Technology SNMP Trap Integration monitor instance based on the results returned by the check.

Each Technology SNMP Trap Integration monitor instance has three status settings:

- **Error if**
- **Warning if**
- **Good if**

You can set unlimited threshold criteria for each status condition per Technology SNMP Trap Integration monitor instance. By default, only one threshold is displayed when you first configure the monitor.

While the monitor is enabled, it is assigned a status of good, warning, or error based on the most recent execution of the monitor action. The measurement taken or the results reported by the monitor are tested against the status threshold settings to determine the status.

The individual results are combined as logical **OR** relationships when more than one threshold condition is defined for any of the three settings. When one or more of the conditions (for example when two conditions for **Error if** setting) are met for a status setting the monitor status is set to the corresponding status condition. If status conditions are met for more than one status setting the status of the monitor is set to the highest valued status condition. For example, if one condition selected as Error if and another condition selected as Warning if are both met, the status would be reported as an error, with **error** being the highest value, **warning** the next highest and **good** the lowest value. The status is displayed by color and a status icon in the SiteScope interface.

A change of status signals an event and acts as a trigger for alerts associated with the monitor or the group to which the monitor belongs.

A change of status may also effect the state of a dependency between monitors. For example, a monitor that detects a change that results in a error status may be a trigger to disable one or more other monitors that are dependent on the SNMP trap data.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement value. You may use the default status thresholds defined for the Technology SNMP Trap Integration or use the following steps to change the monitor status thresholds for this monitor instance:

To edit monitor status thresholds:

1. Use the first drop down menu to for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.

5 Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

Step-by-Step Guide to Integrating SNMP Trap Data into Mercury Business Availability Center

This section provides the overall flow for setting up the Technology SNMP Trap Integration Monitor to work with Mercury Business Availability Center 5.1. If you need more information on performing any of the steps, see the sections on "Setup Requirements" on page 1262, or "Configuring the Technology SNMP Trap Integration Monitor" on page 1264.

To integrate SNMP trap data into Mercury Business Availability Center:

1 Configure the relevant software to send SNMP traps to the SiteScope machine.

2 Open the SiteScope SNMP Trap tool and watch if the traps are received.

If you do not see any traps, make sure that the SNMP trap port is available for the SiteScope: Stop SiteScope, and verify that the SNMP trap port (162) is available—**netstat –na | find "162"** shows no output. (In order to see which

process uses this port, you can download **tcpview** from **www.sysinternals.com**.)

If the port is busy, locate the program that uses it (often the Microsoft SNMP Trap Service) and terminate it. Then restart SiteScope.

3 Save a copy of one of the templates from <SiteScope root directory>\conf\ems\templates to the <SiteScope root directory>\conf\ems\snmptrap directory. For events integration, use the **event.config** template, or for metrics integration, use the **metrics.config** template. It is recommended that you change the name of the .config file copy to include the name of the integrated software, for example: avalon.config.

4 Edit the saved .config file according to the data that you want to see in Mercury Business Availability Center. Each field from the trap is referred to by its name (as it appears in the <SiteScope root directory>\logs\snmptrap.log file), preceded by a dollar sign. For example, use $oid for **oid**, or use $var1 for **var1**. See the section on "Integration Monitor Configuration Files" on page 1049 for more details on the file structure and syntax.

5 Verify that your .config file syntax is correct by running <SiteScope root directory>\conf\ems\tools\test_config.bat <full path to your saved .config file> on the SiteScope machine.

6 Add a Technology SNMP Trap Integration Monitor in Mercury Business Availability Center Monitor Administration, as described in "Configuring the Technology SNMP Trap Integration Monitor" on page 1264. Note the following:

- When adding the new monitor to a group, it is recommended that you use a dedicated group for integration monitors only.
- You add the **Technology SNMP Trap Integration Monitor** from the **Integration Monitors** section in the New SiteScope Monitor pane. If you do not see the **Integration Monitors** section, make sure you have an EMS Option License for your SiteScope.

7 In the New Monitor pane for the Technology SNMP Trap Integration Monitor, make sure that a value is specified for all parameters in the **Main Settings** section.

Note the following:

- **Name** – It is recommended that the monitor name include the name of the integrated software.
- **EMS Configuration File Path** – Enter the full path of the .config file on the SiteScope machine (for example: D:\<SiteScope root directory>\conf\ems\snmptrap\myconfig.config).

8 You can view SNMP traps in the **Tools** link or in <SiteScope root directory\logs\snmptrap.log. (For a better understanding of what SNMP traps are, look at: **www.snmplink.org**)

9 View the data in Mercury Business Availability Center:

- **Events integration** – you can view events in Dashboard (add a Generic EMS source, then add the Generic EMS NodeFactory to a view), System Availability Management Event Log reports, or Analytics. You can also use events when building SLAs.
- **Metrics integration** – you can view the data in any application that supports SiteScope data, including SiteScope reports.
- If you want to watch the incoming samples (to view the original data before it is passed to the applications), use the sprinter utility available under <Mercury Business Availability Center root directory>\bin.

To troubleshoot problems with data arriving to Mercury Business Availability Center, see "Troubleshooting the Technology SNMP Trap Integration Monitor" on page 1274.

Troubleshooting the Technology SNMP Trap Integration Monitor

The following sections provide information on troubleshooting for the Technology SNMP Trap Integration Monitor, and verifying the communication paths:

- "Basic Troubleshooting Guidelines" on page 1275
- "Verify SNMP Trap Reception to SiteScope" on page 1275
- "Common Problems and Solutions" on page 1276

Basic Troubleshooting Guidelines

➤ Check for errors in <SiteScope root directory>\logs\EmsMonitors.log and in <SiteScope root directory>\logs\error.log.

➤ Change the log level to DEBUG in <SiteScope root directory>\conf\log4j.properties, in order to watch outgoing samples.

Change the line:
log4j.category.EmsEventPrinter=${emsloglevel}, ems.appender
to:
log4j.category.EmsEventPrinter= DEBUG, ems.appender.

The log file to look at is:
<SiteScope root directory>\logs\EmsMonitors.log

➤ Use <Mercury Business Availability Center root directory>\bin\sprinter.exe to view sample flow on the bus. Run the executable without parameters in order to get help.

➤ Change the logging level for Dashboard to verify that Dashboard received the samples. Open:
<Mercury Business Availability Center root directory>\conf\log4j4EJB.properties

Change the log level parameter to DEBUG in the following line:
log4j.category.JMDRVSamples=DEBUG,jmdrv.samples.appender

The log file to look at is:
<Mercury Business Availability Center root directory>\log\EJBContainer\TrinitySamples.log

Verify SNMP Trap Reception to SiteScope

You can verify that SiteScope is receiving SNMP traps from other management systems using the SiteScope SNMP Trap Monitor. Use the following steps to verify that SiteScope is receiving traps.

To verify that SiteScope is receiving SNMP traps:

1. Add a SNMP Trap Monitor to SiteScope. In case you already have SNMP Trap Monitor defined, you can skip this step.
2. Configure the intended SNMP Trap sending entity to send traps to the SiteScope machine. The steps to configure the SNMP host depends on

system. Usually, it involves lowering system thresholds to cause normal situations to generate traps. On some systems there is a test mode that you can use to generate traps on demand. The other way is to use one of the freely available SNMP trap generators, and to send copies of the trap to SiteScope.

3 Inspect the SNMP Trap Monitor log file in SiteScope for sent traps. Every SNMP Trap received by the SiteScope will be written into the SNMP Trap Monitor's log file, located in <SiteScope root directory>\logs\snmptrap.log.

Common Problems and Solutions

The following table summarizes common problems and suggested solutions

Problem Symptom	Possible Cause	Solution
The monitor does not appear in the monitor list.	Option License for Integration Monitors had not been provided.	Provide the Option License for Integration Monitors.

The SNMP traps are not forwarded to Mercury Business Availability Center applications.	The SNMP Agent does not emit SNMP traps.	Verify that the SNMP Agent is configured to emit SNMP traps. Use the SiteScope\logs\snmptrap.log file to verify that traps are received by SiteScope. For details, see "Verify SNMP Trap Reception to SiteScope" on page 1275.
	The EMS configuration file contains errors.	Use the SiteScope\conf\ems\tools\test_config.bat tool to verify the EMS configuration file.
	The SNMP trap port is busy.	Make sure that no other SNMP trap service is listening to SNMP traps on the SiteScope machine. Microsoft SNMP Trap Service is common cause on computers running Windows NT or Windows 2000 OS.
	The monitor is not configured to report to these applications.	Make sure that the monitor is configured to report to these applications.
Samples are created and sent from SiteScope, but the data is not seen in Dashboard/Event Log/SiteScope reports.	Samples were dropped due to missing fields or values.	Check in <Mercury Business Availability Center root directory>\log\dispatcher_log.txt.

118

Technology Web Service Integration Monitor

The Technology Web Service Integration Monitor enables a web service entry point to SiteScope. The monitor can be used to report data from third-party Enterprise Management Systems (EMS) to SiteScope through web service. Both event and metrics entry points into Mercury Business Availability Center are published for external systems to use. For each event and/or metric that SiteScope receives, a sample is forwarded to Mercury Business Availability Center containing the event and/or metrics values.

This chapter describes:	On page:
About the Technology Web Service Integration Monitor	1279
Setup Requirements	1281
Configuring the Technology Web Service Integration Monitor	1283
Checking Connectivity to the Technology Web Service Integration Monitor	1289

About the Technology Web Service Integration Monitor

Use the Technology Web Service Integration Monitor for integrating event data or metrics data from your existing EMS system to Mercury Business Availability Center. SiteScope supplies a WSDL file which the user can use to create a client code. The client code reports the event and/or metrics data to SiteScope. The client has four ways in which to report the data to Mercury Business Availability Center as follows:

- report one event

- report an array of events
- report one metric
- report an array of metrics

Note: If you are upgrading SiteScope from version 7.8.1.2 or 7.9.0.0, see the note about upgrading Integration monitor types for version 7.9.1.0 or later in the section "Working with SiteScope Integration Monitors" on page 1043.

What Data Is Collected

The Technology Web Service Integration Monitor collects data that is extracted from any message received by SiteScope report data web service and sends notifications to Mercury Business Availability Center containing preferred values from the original message.

Before setting up the Technology Web Service Integration Monitor, you should understand and map out the purpose and usage of the data that will be forwarded to Mercury Business Availability Center. You should determine if the data will be for presentation in the Dashboard, Service Level Management, and/or reports.

The specific data that is forwarded to Mercury Business Availability Center is controlled by a configuration file for the Technology Web Service Integration Monitor. You use this file to specify the preferred value fields that you want forwarded. There are two general files supplied with this monitor. They are both located in **<SiteScope root directory>\conf\ems\webservice**. The files are **event.config** and **metrics.config**. These files should be reviewed before creating the monitor to verify that the content of the file fits the purpose of the existing integration. For details on the file structure and syntax, see "Integration Monitor Configuration Files" on page 1049.

Note: For information on Integration Monitor logging and troubleshooting, see "Integration Monitor Logging Options" on page 1046 and "Troubleshooting Integration Monitors" on page 1047.

Limitations

If you are working with Mercury Business Availability Center version 5.1 and lower, you cannot define new Technology Web Service Integration monitors or edit existing ones from within Mercury Business Availability Center. If you need to define a new Technology Web Service Integration monitor or edit an existing monitor, you should detach SiteScope from Mercury Business Availability Center, define the monitor in SiteScope's new user interface, and then attach the SiteScope to Mercury Business Availability Center again.

Setup Requirements

The following is an overview of the requirements for using the Technology Web Service Integration Monitor:

- SiteScope must be registered with a Mercury Business Availability Center installation.
- The SiteScope must have a profile defined in the Mercury Business Availability Center installation prior to enabling the registration in the SiteScope interface.
- You need to review the configuration file for the Technology Web Service Integration and determine whether you need to customize it for use with the specific system or application you are monitoring. The configuration file controls what data is to be forwarded to Business Availability Center and is located in **<SiteScope root directory>\conf\ems\webservice**.
- To enable the connection to SiteScope reportMonitorData web service, you must create a client code (in any language) that will make the connection and handle the reporting of the data to SiteScope through the web service.

To create this code, follow the steps in the following procedure.

To enable the connection to SiteScope reportMonitorData web service:

1. Open Explorer and go to the SiteScope link using this address: http://<SiteScope host>:8080/SiteScope/services. Take the WSDL file of the service **reportMonitorData**. The WSDL is an interface file which represents the API of the reportMonitorData web service in SiteScope. The reportMonitorData service is the service that "listens" to incoming messages and forwards them to Mercury Business Availability Center. This file is used to create the client stubs that connect to the service and report the data.
2. Generate the stubs using the WSDL file. The generation of the stubs can be to any language. The way to generate the files depends on the language that you want to use. For example, if you want to use java as the client code, you must use the WSDL2JAVA task in AXIS package which can be downloaded from their Web site. You can run **Java org.apache.axis.wsdl.WSDL2Java <name of saved WSDL file>**. After running this, you get two packages. One package is **com**, which holds the needed objects for sending the data, and the second is **localhost**, which holds the stubs that makes the connection to SiteScope web service.
3. Write the actual client code which uses the generated classes to send the data to SiteScope. In the code, you must call the **setreportMonitorDataEndpointAddress(<SiteScope targetHost>)**, which is found in **MonitorDataAcceptorServiceLocator** (one of the generated stubs) to set the SiteScope address to where you want the data reported.
4. Run your code and check if you get data in the SiteScope Technology Web Service Integration monitor.

Configuring the Technology Web Service Integration Monitor

The Technology Web Service Integration Monitor should be added to a SiteScope monitor group created for this monitor and other Integration Monitor types. It is recommended that you configure Integrations Monitors only after a connection between the SiteScope and Mercury Business Availability Center is established.

Note: SiteScope cannot be deployed behind a firewall. The SiteScope and the monitored system must be on the same LAN or special firewall configuration may be required.

Main Setting for the Technology Web Service Integration Monitor

You use the Main Settings section to specify which events and or metrics are relevant to the monitor and how the monitor creates samples from the entering data using the configuration file.

Name

Enter a text name for this Technology Web Service Integration monitor instance. This text is displayed in the Monitor Administration interface and in the SiteScope interface. If you do not enter a name text, a default name will be used.

System ID

Enter a text system id for this Technology Web Service Integration monitor instance. Each received message from the EMS system holds a system id. Each monitor receives messages only with a system id that matches the system id defined in the monitor. The system id is unique for all Technology Web Service Integration monitors. Enter the system id that represents the messages that you want this monitor to receive.

EMS Configuration File Path

Enter the path to the EMS integration configuration file that you create for this monitor. See the procedure for creating the file in the section "Setup Requirements" on page 1281. For more information about the format of the file see the section on "Integration Monitor Configuration Files" on page 1049. You can store the file in the: **<SiteScope root directory>\conf\ems\webservice** directory.

Advanced Settings for the Technology Web Service Integration Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Technology Web Service Integration Monitor and its display in the product interface. Use this section to set monitor-to-monitor dependencies, customize display options, and configure other settings specific to the Technology Web Service Integration Monitor that may be required in some infrastructure environments. Complete the entries as needed and click the **OK** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Frequency

Select how often the monitor should update its status. The **Frequency** setting for the Technology Web Service Integration Monitor controls only the status reports. The web service data is forwarded when it is received without any delay. The default interval is to update once every 10 minutes. Use the drop-down list to the right of the text box to specify an update interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. You may, however, schedule your monitors to run only on certain days or on a fixed schedule. Click the Edit schedule link to create or edit a monitor schedule. For more information about working with monitor schedules, see the section on Schedule Preferences for Monitoring.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the other monitor should have for the current monitor to run normally. The current monitor will be run normally as long as the monitor selected in the **Depends On** field reports the condition selected in this field. For example, by selecting OK, this monitor is only enabled as long as the monitor selected in the **Depends On** field reports a status of good or OK.

Monitor Description

Enter additional information to describe this monitor. The Monitor Description can include HTML tags such as the <BR>, <HR>, and <B> tags to control display format and style. The description text will appear on the Monitor Detail page.

Report Description

Enter an optional description for this monitor that will make it easier to understand what the monitor does. For example, network traffic or main server response time. This description will be displayed on with each bar chart and graph in Management Reports and appended to the tool-tip displayed when you pass the mouse cursor over the status icon for this monitor on the Monitor Detail page.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. When an error is detected, the monitor will immediately be scheduled to run again once.

Note: In order to change the run frequency of this monitor when an error is detected, you should use the **Error Frequency** option instead of the **Verify Error** option.

Note: The status returned by the **Verify Error** run of the monitor will replace the status of the originally scheduled run that detected an error. This may cause the loss of important performance data if the data from the verify run is different than the initial error status.

Use of this option across many monitor instances may result in significant monitoring delays in the case that multiple monitors are rescheduled to verify errors at the same time.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the status of this Technology Web Service Integration monitor instance based on the results returned by the check.

Each Technology Web Service Integration monitor instance has three status settings:

- **Error if**
- **Warning if**
- **Good if**

You can set unlimited threshold criteria for each status condition per Technology Web Service Integration monitor instance. By default, only one threshold is displayed when you first configure the monitor.

While the monitor is enabled, it is assigned a status of good, warning, or error based on the most recent execution of the monitor action. The measurement taken or the results reported by the monitor are tested against the status threshold settings to determine the status.

The individual results are combined as logical **OR** relationships when more than one threshold condition is defined for any of the three settings. When one or more of the conditions (for example when two conditions for **Error if** setting) are met for a status setting the monitor status is set to the corresponding status condition. If status conditions are met for more than one status setting the status of the monitor is set to the highest valued status condition. For example, if one condition selected as Error if and another condition selected as Warning if are both met, the status would be reported as an error, with **error** being the highest value, **warning** the next highest and **good** the lowest value. The status is displayed by color and a status icon in the SiteScope interface.

A change of status signals an event and acts as a trigger for alerts associated with the monitor or the group to which the monitor belongs.

A change of status may also effect the state of a dependency between monitors. For example, a monitor that detects a change that results in a error status may be a trigger to disable one or more other monitors that are dependent on the web service data.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement value. You may use the default status thresholds defined for the Technology Web Service Integration or use the following steps to change the monitor status thresholds for this monitor instance:

To edit monitor status thresholds:

1. Use the first drop down menu to for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.

5 Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

Checking Connectivity to the Technology Web Service Integration Monitor

After creating a Technology Web Service Integration monitor in SiteScope, you can check connectivity to the web service by using the **test_client** which is located in the **<SiteScope root directory>\conf\ems\webservice\test_client** directory. This tool sends constant messages to SiteScope reportMonitorData web service. The messages can be either metrics messages or event messages.

To use the client tool to check connectivity:

1 In the **<SiteScope root directory>\conf\ems\webservice\test_client** directory, run the **test_event_client.bat** for events or **test_metrics_client.bat** for metrics, using the following parameters:

- **Target Host** – the address of the SiteScope host which receives the messages.
- **Number of messages to send** – Number of messages to send to SiteScope.
- **System Id** – System Id of the monitor that receives the messages.
- **Severity/Quality** – Severity of the event when forwarding events (default is to send 1 to 5). Quality of the metric when forwarding metrics data (default is 0-3).

2 If you are forwarding other values to Mercury Business Availability Center, you must edit the configuration file accordingly.

The tool can also be executed with no parameters. In this case, the tool tries to send one message to the local host. The message has the system id: **Test Event System Id**. The severity is 5 (for events) or the quality is 3 (for metrics).

If you use this option, you must activate it on the SiteScope machine and have a Technology Web Service Integration monitor with the system id: **Test Event System Id**.

3 After running the tool, go to the appropriate SiteScope monitor and see if the number of messages received equals the number that you sent. In addition, you can go to one of the applications (Dashboard, System Availability Management) and see if the data that you sent is displayed.

119

Tivoli DM Metrics Monitor

You use the Tivoli DM Metrics Monitor to integrate data collected by Tivoli Endpoint Monitors into Mercury Business Availability Center.

This chapter describes:	On page:
About the Tivoli DM Metrics Monitor	1291
Setup Requirements	1292
Configuring the Tivoli DM Metrics Monitor	1293

Note: Metrics that do not have a numeric value are not reported to Mercury Business Availability Center.

About the Tivoli DM Metrics Monitor

You use the Tivoli DM Metrics Monitor to collect metrics monitored by a Tivoli DM engine running on any platform supporting Tivoli Endpoint. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning.

The Tivoli DM Metrics Monitor can now accept a regular expression to identify a server, as well as the server name itself. By using regular expressions to match server names, you can deploy one instance of a Tivoli DM Metrics Monitor to monitor multiple servers.

The Tivoli DM Metrics monitor uses a pre-defined configuration file to define the processing of incoming data and define the output sample forwarded to Mercury Business Availability Center. If you have to make any specific customizations, you can modify this configuration file. For details, see "Integration Monitor Configuration Files" on page 1049.

Note: For information on Integration Monitor logging and troubleshooting, see Integration Monitor Logging Options and Troubleshooting Integration Monitors in Chapter 101, "Working with SiteScope Integration Monitors."

Note: If you are upgrading SiteScope from version 7.8.1.2 or 7.9.0.0, see the note about upgrading Integration Monitor types for version 7.9.1.0 or later in the section "Working with SiteScope Integration Monitors" on page 1043.

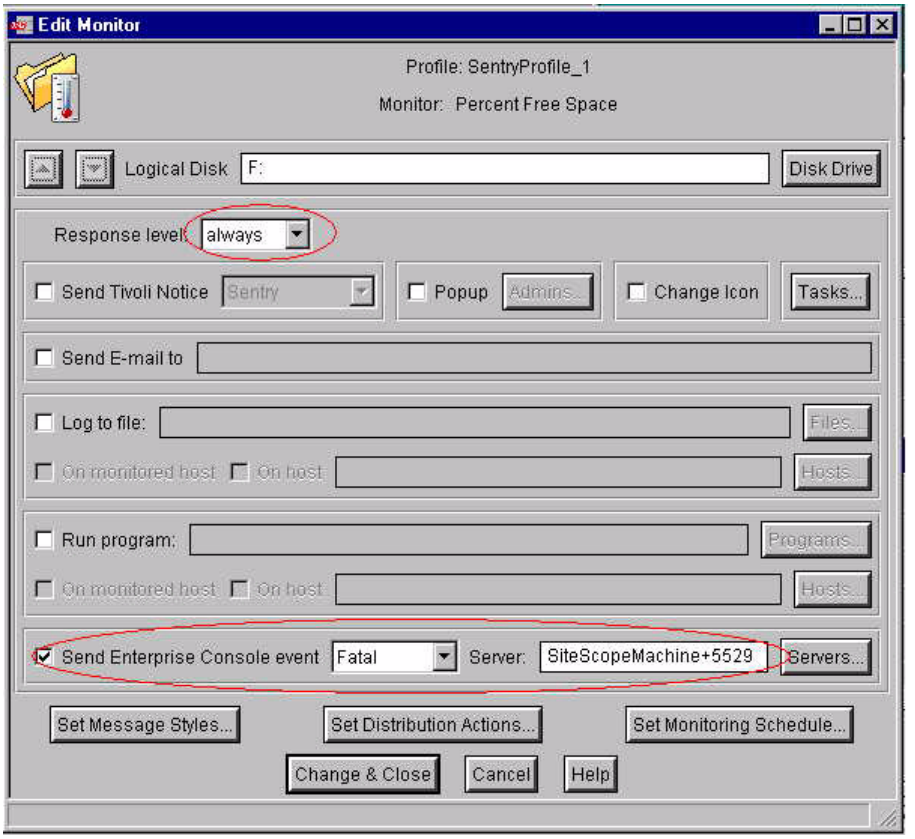
Setup Requirements

The Tivoli DM Passive Monitor listens for incoming TEC SENTRY events and extracts from it sampled data. Tivoli Sentry profiles need to be changed in order to post the desired metrics to the monitor in the form of TEC event. By default the monitor listens for incoming events on TCP port 5529.

To configure the Tivoli Sentry profile:

1. Open the profile definition
2. Open the desired monitor definition
3. Add Send Enterprise Console event respond and set up parameters of the SiteScope host and Tivoli DM Passive Monitor port in the Server field in the format <Hostname> + <PortNumber>
4. Repeat steps 2-3 for all desired counters
5. Save and distribute the profile

The following is an example display of the Tivoli DM Edit Monitor Window:



Configuring the Tivoli DM Metrics Monitor

The Tivoli DM Metrics Monitor should be added to a SiteScope monitor group created for this monitor and other Integration Monitor types. It is recommended that you configure Integrations Monitors only after a connection between the SiteScope and Mercury Business Availability Center is established.

Note: SiteScope cannot be deployed behind a firewall. The SiteScope and the monitored system must be on the same LAN or special firewall configuration may be required.

Main Settings for the Tivoli DM Metrics Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the Tivoli DM system data and the text name used for this monitor instance in the interface. Complete the entries in the Main Settings section as described below. Complete the entries as needed and click the **OK** button to save the settings.

Name

Enter a text name for this Tivoli DM Metrics monitor instance. This text is displayed in the Monitor Administration interface and in the SiteScope interface. If you do not enter a name text, a default name will be used.

Server

Enter the server name on which the Tivoli server you want to monitor is running. You can also enter a regular expression which matches multiple server names of the servers you want to monitor. For example:

- To match any server that is configured to send metrics to SiteScope, use: .*
- To match all the servers that starts with the sequence "abc", use: (abc).*
- To match all the servers that starts with the sequence "abc" and ends with a number, use: (abc).*[0-9]

Monitor Port

Enter the port number on which the Tivoli DM Metrics monitor listens for incoming metrics from Tivoli endpoints. By default this field is set to 5529.

Advanced Settings for the Tivoli DM Metrics Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Tivoli DM Metrics Monitor and its display in the product interface. Use this section to set monitor-to-monitor dependencies, customize display options, and configure other settings specific to the Tivoli DM Metrics Monitor that may be required in some infrastructure environments. Complete the entries as needed and click the **OK** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

EMS Configuration File Path

Enter the path to the EMS integration configuration file relative to the SiteScope installation. The default location is: <SiteScope root directory>\conf\ems\tivoli\metrics.config. For more information about the format of the file see the section "Integration Monitor Configuration Files" on page 1049.

If you want to edit this file, create a copy on the SiteScope machine and work in the new copy. Then, in Monitor Administration, edit the path to the file.

Frequency

Select how often the monitor should update its status. The **Frequency** setting for the Tivoli DM Metrics Monitor controls only the status reports. The Tivoli DM system data are forwarded when they are received without any delay. The default interval is to update once every 10 minutes. Use the drop-down list to the right of the text box to specify an update interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. You may, however, schedule your monitors to run only on certain days or on a fixed schedule. Click the Edit schedule link to create or edit a monitor schedule. For more information about working with monitor schedules, see the section on Schedule Preferences for Monitoring.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the other monitor should have for the current monitor to run normally. The current monitor will be run normally as long as the monitor selected in the **Depends On** field reports the condition selected in this field. For example, by selecting OK, this monitor is only enabled as long as the monitor selected in the **Depends On** field reports a status of good or OK.

Monitor Description

Enter additional information to describe this monitor. The Monitor Description can include HTML tags such as the <BR>, <HR>, and <B> tags to control display format and style. The description text will appear on the Monitor Detail page.

Report Description

Enter an optional description for this monitor that will make it easier to understand what the monitor does. For example, network traffic or main server response time. This description will be displayed on with each bar chart and graph in Management Reports and appended to the tool-tip displayed when you pass the mouse cursor over the status icon for this monitor on the Monitor Detail page.

EMS Time Difference

Use this option to account for time differences between the system clock time on the monitored EMS machine and the server where SiteScope is running. This is only needed when the EMS data includes time data and the time data shows that there is a time difference between the EMS machine and the SiteScope server. If the time difference is too great the data may be discarded from Mercury Business Availability Center.

Note: The time difference value only needs to be entered if the difference is greater than one minute. There is no need to synchronize differences of seconds less than one minute.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. When an error is detected, the monitor will immediately be scheduled to run again once.

Note: In order to change the run frequency of this monitor when an error is detected, you should use the **Error Frequency** option instead of the **Verify Error** option.

Note: The status returned by the **Verify Error** run of the monitor will replace the status of the originally scheduled run that detected an error. This may cause the loss of important performance data if the data from the verify run is different than the initial error status.

Use of this option across many monitor instances may result in significant monitoring delays in the case that multiple monitors are rescheduled to verify errors at the same time.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the status settings to set threshold conditions that determine the status of this Tivoli DM Metrics monitor instance based on the results returned by the check.

Each Tivoli DM Metrics monitor instance has three status settings:

- **Error if**
- **Warning if**
- **Good if**

While the monitor is enabled, it is assigned a status of good, warning, or error based on the most recent execution of the monitor action. The measurement taken or the results reported by the monitor are tested against the status threshold settings to determine the status. The status is displayed by color and a status icon in the SiteScope interface.

A change of status acts as a trigger for alerts associated with the monitor or the group to which the monitor belongs. For example, if the Tivoli DM Metrics Monitor detects that the Tivoli DM system data has become unavailable, the status change from good to error is used to trigger an alert on error.

A change of status may also effect the state of a dependency between monitors.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement value. You may use the default status thresholds defined for the Tivoli DM Metrics or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop down menu to for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. Repeat these steps for the Warning if and Good if settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

120

Tivoli TEC Event Monitor

Use the Tivoli TEC Event Monitor to monitor the number of events received by a particular Tivoli Event Server and forward them to Mercury Business Availability Center. This monitor supports Tivoli DM versions 3.6, 3.7, 3.8, and 3.9 installed on any operating system. The monitor also supports ITM version 5.1.1 for events only.

This chapter describes:	On page:
About the Tivoli TEC Event Monitor	1301
Integration Architecture	1302
System Requirements	1303
Configuring the Tivoli TEC Event Monitor	1304

About the Tivoli TEC Event Monitor

The Tivoli TEC Event Monitor listens for incoming TEC events and reports the total number of received events and number of received events per minute. You can forward TEC events to a Mercury Business Availability Center platform for further use by Mercury Business Availability Center applications. For details, see the Advanced Options section below.

The Tivoli TEC Event monitor uses a pre-defined configuration file to define the processing of incoming data and define the output sample forwarded to Mercury Business Availability Center. If you have to make any specific customizations, you can modify this configuration file. For details, see “Integration Monitor Configuration Files” on page 1049.

Note: For information on Integration Monitor logging and troubleshooting, see "Integration Monitor Logging Options" on page 1046 and "Troubleshooting Integration Monitors" on page 1047.

Note: If you are upgrading SiteScope from version 7.8.1.2 or 7.9.0.0, see the note about upgrading Integration Monitor types for version 7.9.1.0 or later in the section "Working with SiteScope Integration Monitors" on page 1043.

Integration Architecture

Tivoli TEC integration architecture is based on TCP communication and on Tivoli TEC rule-based, event-forwarding capability. To integrate SiteScope with Tivoli TEC, you must define additional rules on the TEC server. These rules handle different types of custom events from the SiteScope Tivoli TEC monitor to maintain integration.

Events sent from SiteScope to the Tivoli TEC server include:

- **Topaz_ProbeDisconnect** – sent each time the monitor refreshes itself and indicates to the TEC server that it can stop forwarding events to SiteScope.
- **Topaz_ProbeConnect** – sent each time the monitor refreshes itself after Topaz_ProbeDisconnect events have been sent. This event indicates to the TEC server that SiteScope is connected and events can be forwarded to it.
- **Topaz_ProbeHeartbeat** – sent on a schedule of every minute to indicate that SiteScope is running and that events can be forwarded to it. If a Topaz_ProbeHeartbeat event has not been sent for more than five minutes, the TEC server stops forwarding events to SiteScope.

System Requirements

You need to configure your Tivoli Event Server to forward events to a SiteScope machine. The configuration is performed by creating new rule in the TEC Event Server rule base. If you are a seasoned Tivoli Administrator, you can perform the configuration manually.

The following are the recommended steps to configure the TEC Event Server.

Note: For the following steps you must have at least `senior` Tivoli authorization.

---

1. Make available the contents of the `SiteScope/ems/Tivoli/rulebase/`*`tec_version_number`* directory to your TEC server where *`tec_version_number`* is replaced with the TEC version number you are monitoring (for example, `tec37`). You can copy the directory locally to the server or map/mount the network drive.
2. Open a command prompt (or new terminal) window. Initialize the Tivoli environment by running Tivoli script. If the TEC server machine is running on NT/2000 server, the script is located under: `% SystemRoot%\ system32\ drivers\ etc\ Tivoli\ setup_ env. cmd`. If the TEC server is running on UNIX machine, run the script: `/ etc/ Tivoli/ setup. sh`
3. Run the SiteScope rule base installation Perl script: `perl pcreate` {`SiteScope Hostname`} {`Rule Base Path`},on your TEC event server, where {`SiteScope Hostname`} is the name of the SiteScope machine and {`Rule Base Path` } is the full path for the TopazProbe rule base creation. Note that if you run the script without parameters you will be asked for the required parameters.

   The TopazProbe rule base creation performs the following tasks on the TEC server:

1. Creates a new TopazProbe rule base.

2. Imports into it the Mercury Business Availability Center probe event class definition and rules.
3. Imports the active rule base content (event class definitions, rule sets and targets) into the TopazProbe rule base.
4. Activate TopazProbe rule base.
5. Restarts the event server.

Note: If you made changes to the default Tivoli event definition (for example, **root.baroc, tec.baroc**) you will need to copy the modified files manually from the active rulebase to the new rulebase before compiling the new rulebase.

You can use the TEC Event History tool to view recent TEC events received by the TEC event listener included with SiteScope.

The default run schedule for this monitor is every 10 minutes, but you can change it to run more or less often using the **Frequency** setting. It is recommended to set up monitor scheduling to match the appropriate Tivoli Event Server scheduling.

Configuring the Tivoli TEC Event Monitor

The Tivoli TEC Event Monitor should be added to a SiteScope monitor group created for this monitor and other Integration Monitor types. It is recommended that you configure Integrations Monitors only after a connection between the SiteScope and Mercury Business Availability Center is established.

Note: SiteScope cannot be deployed behind a firewall. The SiteScope and the monitored system must be on the same LAN or special firewall configuration may be required.

Main Settings for the Tivoli TEC Event Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the Tivoli TEC system event data, how often this Tivoli TEC Event Monitor instance should be run, and the text name used for this monitor instance in the interface. Complete the entries in the Main Settings section as described below. Complete the entries as needed and click the **OK** button to save the settings.

Name

Enter a text name for this Tivoli TEC Event monitor instance. This text is displayed in the Monitor Administration interface and in the SiteScope interface. If you do not enter a name text, a default name will be used.

TEC Server

Enter the TEC Server hostname and port number in form `hostname:port`. Upon monitor definition `Topaz_ProbeConnect` event will be sent to the specified TEC event server/port. If the TEC server runs on UNIX platform and uses portmaper service leave unspecified port number and monitor will obtain the port number from portmaper service on TEC machine. Every minute the monitor sends `Topaz_ProbeHeartBeat` event to the same destination and `Topaz_Probe Disconnect` upon monitor deletion. Rules created in TopazProbe rule base will automatically detects whether incoming event should be forwarded to SiteScope. For example, if your TEC server runs on NT machine named `tivoli01` and listens for incoming non TME events on port 5529 specify `tivoli01:5529.` If the TEC server runs on UNIX machine `tivoli02` and uses portmaper specify `tivoli02.`

If you leave the parameter unspecified the monitor reports Total Number of Events and Number of Events per minute received from any location.

Monitor Port

Enter the port number on which the Tivoli TEC Event monitor listens for incoming events from Tivoli endpoints. By default this field is set to 5529.

Advanced Settings for the Tivoli TEC Event Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Tivoli TEC Event Monitor and its display in the product interface. Use this section to set monitor-to-monitor dependencies, customize display options, and configure other settings specific to the Tivoli TEC Event Monitor that may be required in some infrastructure environments. Complete the entries as needed and click the **OK** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

EMS Configuration File Path

Enter the path to the EMS integration configuration file relative to the SiteScope installation. The default location is: <SiteScope root directory>\conf\ems\tivoli\event.config. For more information about the format of the file see the section "Integration Monitor Configuration Files" on page 1049.

If you want to edit this file, create a copy on the SiteScope machine and work in the new copy. Then, in Monitor Administration, edit the path to the file.

Frequency

Select how often the monitor should update its status. The **Frequency** setting for the Tivoli TEC Event Monitor controls only the status reports. The Tivoli TEC system event data are forwarded when they are received without any delay. The default interval is to update once every 10 minutes. Use the drop-down list to the right of the text box to specify an update interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. You may, however, schedule your monitors to run only on certain days or on a fixed schedule. Click the Edit schedule link to create or edit a monitor schedule. For more information about working with monitor schedules, see the section on Schedule Preferences for Monitoring.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the other monitor should have for the current monitor to run normally. The current monitor will be run normally as long as the monitor selected in the **Depends On** field reports the condition selected in this field. For example, by selecting OK, this monitor is only enabled as long as the monitor selected in the **Depends On** field reports a status of good or OK.

Monitor Description

Enter additional information to describe this monitor. The Monitor Description can include HTML tags such as the <BR>, <HR>, and <B> tags to control display format and style. The description text will appear on the Monitor Detail page.

Report Description

Enter an optional description for this monitor that will make it easier to understand what the monitor does. For example, network traffic or main server response time. This description will be displayed on with each bar chart and graph in Management Reports and appended to the tool-tip displayed when you pass the mouse cursor over the status icon for this monitor on the Monitor Detail page.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. When an error is detected, the monitor will immediately be scheduled to run again once.

Note: In order to change the run frequency of this monitor when an error is detected, you should use the **Error Frequency** option instead of the **Verify Error** option.

Note: The status returned by the **Verify Error** run of the monitor will replace the status of the originally scheduled run that detected an error. This may cause the loss of important performance data if the data from the verify run is different than the initial error status.

Use of this option across many monitor instances may result in significant monitoring delays in the case that multiple monitors are rescheduled to verify errors at the same time.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the status of this Tivoli TEC Event monitor instance based on the results returned by the check.

Each Tivoli TEC Event monitor instance has three status settings:

- **Error if**
- **Warning if**
- **Good if**

You can set unlimited threshold criteria for each status condition per Tivoli TEC Event monitor instance. By default, only one threshold is displayed when you first configure the monitor.

While the monitor is enabled, it is assigned a status of good, warning, or error based on the most recent execution of the monitor action. The measurement taken or the results reported by the monitor are tested against the status threshold settings to determine the status.

The individual results are combined as logical **OR** relationships when more than one threshold condition is defined for any of the three settings. When one or more of the conditions (for example when two conditions for **Error if** setting) are met for a status setting the monitor status is set to the corresponding status condition. If status conditions are met for more than one status setting the status of the monitor is set to the highest valued status condition. For example, if one condition selected as Error if and another condition selected as Warning if are both met, the status would be reported as an error, with **error** being the highest value, **warning** the next highest and **good** the lowest value. The status is displayed by color and a status icon in the SiteScope interface.

A change of status signals an event and acts as a trigger for alerts associated with the monitor or the group to which the monitor belongs.

A change of status may also effect the state of a dependency between monitors. For example, a monitor that detects a change that results in a error status may be a trigger to disable one or more other monitors that are dependent on the Tivoli TEC system event data.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement value. You may use the default status thresholds defined for the Tivoli TEC Event or use the following steps to change the monitor status thresholds for this monitor instance:

To edit monitor status thresholds:

1. Use the first drop down menu to for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop down menu to select the comparison operator(s) that will define the status threshold.

3 Enter a value applicable to the measurement parameter in the third text box.

4 To add another threshold setting, click the **New Error If** button and repeat the steps above.

5 Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

121

WhatsUp Event Monitor

The WhatsUp Event Monitor watches for reports on availability of hosts and services that are issued by WhatsUp Gold, a discovery and monitoring tool for TCP/IP, IPX, and NetBIOS networks, and forwards that data to Mercury Business Availability Center. This monitor enables you to monitor WhatsUp Gold version 8.0 installed on any operating system.

This chapter describes:	On page:
About the WhatsUp Event Monitor	1313
Configuring the WhatsUp Event Monitor	1314

About the WhatsUp Event Monitor

Use the WhatsUp Event Monitor to integrate WhatsUp Gold alerts on the current condition of hosts and services in a WhatsUp Event Monitored network. WhatsUp Gold allows the user to define the network topology by creating network maps and then to specify their physical and logical connections. WhatsUp Gold can be configured to write the alerts it generates to a log file. In addition, you can be notified of early warning conditions before something more serious happens.

The WhatsUp Event Monitor receives alerts from the WhatsUp logs. Thus it must have network access to the machine where the WhatsUp Gold logs are stored. The logs can be accessed using the **WhatsUp Installation Directory** if WhatsUp Gold is running on the same machine as SiteScope (not recommended), or through a UNC path if WhatsUp Gold is running on a remote NT/2000 machine. When using a UNC path, the root directory on the remote machine in that path must be shared. To monitor on a remote UNIX machine, define a UNIX remote to the WhatsUp machine and then select that machine using the **Server** selection link.

The WhatsUp Event monitor uses a pre-defined configuration file to define the processing of incoming data and define the output sample forwarded to Mercury Business Availability Center. If you have to make any specific customizations, you can modify this configuration file. For details, see "Integration Monitor Configuration Files" on page 1049.

Note: For information on Integration Monitor logging and troubleshooting, see "Integration Monitor Logging Options" on page 1046 and "Troubleshooting Integration Monitors" on page 1047.

Note: If you are upgrading SiteScope from version 7.8.1.2 or 7.9.0.0, see the note about upgrading Integration monitor types for version 7.9.1.0 or later in the section "Working with SiteScope Integration Monitors" on page 1043.

Configuring the WhatsUp Event Monitor

The WhatsUp Event Monitor should be added to a SiteScope monitor group created for this monitor and other Integration Monitor types. It is recommended that you configure Integrations Monitors only after a connection between the SiteScope and Mercury Business Availability Center is established.

Note: SiteScope cannot be deployed behind a firewall. The SiteScope and the monitored system must be on the same LAN or special firewall configuration may be required.

Main Settings for the WhatsUp Event Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the WhatsUp system for event data, how often this WhatsUp Event Monitor instance should be run, and the text name used for this monitor instance in the interface. Complete the entries in the Main Settings section as described below. Complete the entries as needed and click the **OK** button to save the settings.

Name

Enter a text name for this WhatsUp Event monitor instance. This text is displayed in the Monitor Administration interface and in the SiteScope interface. If you do not enter a name text, a default name will be used.

Frequency

Select how often the monitor should update its status. The **Frequency** setting for the WhatsUp Event Monitor controls only the status reports. The WhatsUp system for event data are forwarded when they are received without any delay. The default interval is to update once every 10 minutes. Use the drop-down list to the right of the text box to specify an update interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Servers

Choose the server where the WhatsUp Event log you want to monitor is located. Use the drop-down list to select a server from the list of remote servers that are available to the SiteScope agent.

Log File Encoding

Specify the log file encoding. In the WhatsUp Event log, this field should remain with its default value.

WhatsUp Installation Directory

Enter the path to the WhatsUp Gold installation directory where the *.tab log files are located. WhatsUp Gold logs changes once a week and the WhatsUp Event Monitor can generate the current log file name according to the installation directory and date.

Note: If you are using SSH as a connection method to remote NT servers, you will need to select the remote server using the **Server** selection above. It is not necessary to select a remote NT server if you are using NetBIOS to connect to remote NT servers.

Advanced Settings for the WhatsUp Event Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the WhatsUp Event Monitor and its display in the product interface. Use this section to set monitor-to-monitor dependencies, customize display options, and configure other settings specific to the WhatsUp Event Monitor that may be required in some infrastructure environments. Complete the entries as needed and click the **OK** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

No Error if File Not Found

Check this box if you want this monitor to remain in GOOD status, if the file is not found.

EMS Configuration File Path

Enter the path to the EMS integration configuration file relative to the SiteScope installation. The default location is: <SiteScope root directory>\conf\ems\whatsup\event.config. For more information about the format of the file see the section "Integration Monitor Configuration Files" on page 1049.

If you want to edit this file, create a copy on the SiteScope machine and work in the new copy. Then, in Monitor Administration, edit the path to the file.

Run Alerts

Choose the method for running alerts for this monitor. If the **for each log entry matched** option is chosen, then the monitor triggers alerts for every matching entry found and the monitor will remain "good". If the **once, after all log entry have been checked** option is chosen, then the monitor counts up the number of matches and then triggers alerts based on the **Error If** and **Warning If** thresholds defined for the monitor.

Note: When the WhatsUp Event Monitor is run in the for each event matched alert method, the monitor will never report a status of error or warning, regardless of the results of the content match or even if the target log file is not found.

Content Match

The default content match for the monitor will match log file entries for the following four types of alerts:

- service is down (default severity warning)
- service is up (default severity normal)
- host is down (default severity critical)
- host is up (default severity normal)

You can use a different expression by entering the text to look for in the log entries in this text box. Regular expressions may also be used in this box to match text patterns. Unlike the content match feature of other SiteScope monitors, the WhatsUp Event Monitor content match is run repeatedly against the most recent content of target log file until all matches are found. This means the monitor sends each matched line to MercuryAM as an event sample and also reports how many times the matched pattern was found.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. You may, however, schedule your monitors to run only on certain days or on a fixed schedule. Click the Edit schedule link to create or edit a monitor schedule. For more information about working with monitor schedules, see the section on Schedule Preferences for Monitoring.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the other monitor should have for the current monitor to run normally. The current monitor will be run normally as long as the monitor selected in the **Depends On** field reports the condition selected in this field. For example, by selecting OK, this monitor is only enabled as long as the monitor selected in the **Depends On** field reports a status of good or OK.

Monitor Description

Enter additional information to describe this monitor. The Monitor Description can include HTML tags such as the <BR>, <HR>, and <B> tags to control display format and style. The description text will appear on the Monitor Detail page.

Report Description

Enter an optional description for this monitor that will make it easier to understand what the monitor does. For example, network traffic or main server response time. This description will be displayed on with each bar chart and graph in Management Reports and appended to the tool-tip displayed when you pass the mouse cursor over the status icon for this monitor on the Monitor Detail page.

EMS Time Difference

Use this option to account for time differences between the system clock time on the monitored EMS machine and the server where SiteScope is running. This is only needed when the EMS data includes time data and the time data shows that there is a time difference between the EMS machine and the SiteScope server. If the time difference is too great the data may be discarded from Mercury Business Availability Center.

Note: The time difference value only needs to be entered if the difference is greater than one minute. There is no need to synchronize differences of seconds less than one minute.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. When an error is detected, the monitor will immediately be scheduled to run again once.

Note: In order to change the run frequency of this monitor when an error is detected, you should use the **Error Frequency** option instead of the **Verify Error** option.

Note: The status returned by the **Verify Error** run of the monitor will replace the status of the originally scheduled run that detected an error. This may cause the loss of important performance data if the data from the verify run is different than the initial error status.

Use of this option across many monitor instances may result in significant monitoring delays in the case that multiple monitors are rescheduled to verify errors at the same time.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the status of this WhatsUp Event monitor instance based on the results returned by the check.

Each WhatsUp Event monitor instance has three status settings:

- **Error if**
- **Warning if**
- **Good if**

You can set unlimited threshold criteria for each status condition per WhatsUp Event monitor instance. By default, only one threshold is displayed when you first configure the monitor.

While the monitor is enabled, it is assigned a status of good, warning, or error based on the most recent execution of the monitor action. The measurement taken or the results reported by the monitor are tested against the status threshold settings to determine the status.

The individual results are combined as logical **OR** relationships when more than one threshold condition is defined for any of the three settings. When one or more of the conditions (for example when two conditions for **Error if** setting) are met for a status setting the monitor status is set to the corresponding status condition. If status conditions are met for more than one status setting the status of the monitor is set to the highest valued status condition. For example, if one condition selected as Error if and another condition selected as Warning if are both met, the status would be reported as an error, with **error** being the highest value, **warning** the next highest and **good** the lowest value. The status is displayed by color and a status icon in the SiteScope interface.

A change of status signals an event and acts as a trigger for alerts associated with the monitor or the group to which the monitor belongs.

A change of status may also effect the state of a dependency between monitors. For example, a monitor that detects a change that results in a error status may be a trigger to disable one or more other monitors that are dependent on the WhatsUp system for event data.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement value. You may use the default status thresholds defined for the WhatsUp Event or use the following steps to change the monitor status thresholds for this monitor instance:

To edit monitor status thresholds:

1. Use the first drop down menu to for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.
5. Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For more information see "Working with Categories" in *Working with Monitor Administration*.

122

Integration with HP Network Node Manager

Mercury Business Availability Center can accept events from Hewlett Packard Network Node Manager (NNM).

This chapter describes:	On page:
About Network Node Manager Integration	1325
Writing Scripts to Export Network Node Manager Data	1326
Configuring Events in Network Node Manager	1326

About Network Node Manager Integration

You can forward from Network Node Manager (NNM) event data by configuring NNM to run a script for each event that you want forwarded to Mercury Business Availability Center. The script that you write and associate with NNM can do one of the following actions:

- Write the NNM data to a log file
- Send an SNMP trap with the NNM data to a SiteScope server

If your script writes the data to a log you then use a Technology Log File Integration Monitor to read the data and forward it to Mercury Business Availability Center. If you use a script to send an SNMP trap to a SiteScope server, you use an Technology SNMP Trap Integration Monitor configured to receive it and forward to Mercury Business Availability Center.

Writing Scripts to Export Network Node Manager Data

The script you use should accept data from Network Node Manager as a command line argument, and process the data so that it can be forwarded to Mercury Business Availability Center. The following sections describe example scripts that can be used to export NNM data.

Example Script for Writing to a Log File

The following Perl script receives data from the command line and writes it to a log file as a comma separated vector of values that can be parsed by the Log File Integration Monitor:

```
#!/usr/bin/perl
open LOG, ">>log1.log" or die;
print LOG (join ',', @ARGV) . "\n";
close LOG;
```

Example Script for Sending SNMP Trap Data

The following Perl script receives data from the command line and sends it as a message in an SNMP trap (using SNMP data generated by Network Node Manager) that can be caught by a Technology SNMP Trap Integration Monitor. It accepts the host name to which the trap is sent as the first parameter and a string description of the alert as the second parameter.

```
#!/usr/bin/perl
$host = $ARGV[0];
$message = $ARGV[1];
system("snmptrap $host \"\" \"\" 6 0 5 system.sysDescr.0 “ .
“octetstringascii $message");
```

Configuring Events in Network Node Manager

Use the following steps to configure Network Node Manager to execute a script for the requested events in Network Node Manager. The figure below shows examples of the applicable Network Node Manager screens and dialogs you use.

To configure Network Node Manager to execute scripts

1. From the **Options** menu choose **Event Configuration.**
2. Select the requested enterprise and event from the **Event Configuration** dialog.
3. Select the Actions tab from the Edit > Events > Modify Events dialog.
4. Type the command line for the script in the **Command for Automatic Action** text box. You may use NNM variables to pass data to the command line.
5. Press **OK** to close the **Modify Events** dialog.
6. From the **File** menu in the **Event Configuration** dialog select **Save**.

Part VI

Monitor Troubleshooting Tools

123

Tools for Troubleshooting

When SiteScope reports a problem with a monitored system or you are having difficulty configuring a monitor, it is useful to have some resources you can use to troubleshoot and diagnose problems. SiteScope provides a number of tools to help you uncover issues and facilitate monitor configuration.

This chapter describes:	On page:
About SiteScope Tools	1331
Working with SiteScope Tools	1333

About SiteScope Tools

The SiteScope Tools node contains a number of utilities that are useful to test the monitoring environment. You can use these tools to make a variety of requests and queries of systems you are trying to monitor and view detailed results of the action. This may include simply testing network connectivity or verifying login authentication for accessing an external database or service.

The following tables list diagnostic tools that are available. See the applicable sections for more information about these tools.

Application Diagnostic Tools

Tool Name	Description
DNS Lookup	Test a DNS server to verify that it can resolve a domain name. (Includes access to a Traceroute tool to test network routing.)
Database Connection	Check connectivity and configuration of JDBC or ODBC database connections.
FTP Server	Check the availability of an FTP server and whether a file can be retrieved.
Get URL and URL Content	Requests a URL from a server and prints the returned data. (Includes access to a Trace Route tool to test network routing.)
Mail Round Trip Test	Test a mail server by sending and retrieving a test message.
Ping	Performs a round-trip Ping test across the network. (Includes access to a Traceroute tool to test network routing.)
SNMP Browser Tool	Browse an SNMP MIB and view available OIDs.
SNMP	Performs a SNMP get command to a specified SNMP host to retrieve a list of OIDs.
SNMP Trap	View the log of SNMP Traps received by SiteScope from SNMP-enabled devices.
Check URL Sequence	Retrieve a sequence of URLs.
Web Service	Used to test the availability of SOAP enabled Web Services.
XML Transform Test	Test custom XSL transformation of XML data to be monitored with the Browsable XML Monitor.

Server Diagnostic Tools

Tool Name.	Description
Network	Display the server's network interface status and active connections
Processes	Shows a list of currently running processes either locally or on a remote server
Services	Shows a list of currently running Windows Services.

Advanced Diagnostic Tools

Tool Name	Description
News Server	Check whether a News Server is operational.
Event Log	Display portions of the Windows Event Log locally or on a remote server.
LDAP Authentication Test	Test an LDAP server by requesting an user authentication.
Performance Counters	Check connectivity to and values in Win NT Performance Counter registries.
Regular Expression Test	Test a regular expression for content matching against a sample of the content you want to monitor.
TEC Event History	Show a list of Tivoli TEC events recently received by SiteScope (requires additional licensing).

Working with SiteScope Tools

You access the SiteScope Tools by expanding the Tools node in the left menu tree and then clicking on the icon or name for the tool you want to use. The tool form is displayed in the Contents area.

The following sections describe how to use each of the SiteScope diagnostic tools.

Database Connection

The Database Connection diagnostic tool is used to test and verify connectivity between SiteScope and an external ODBC or JDBC compatible database. which uses a supplied JDBC or ODBC driver and URL Connection string to test the connection to a database. This diagnostic tool will check to see if:

- the supplied database driver can be found and loaded
- a connection can be made to the database
- an optional SQL query can be executed and the results displayed
- the database connection and resources can be closed

If exceptions or errors occur during the test, the information is printed along with suggested actions to help with troubleshooting. This tool can be useful in verifying connection parameter values needed to setup Database monitors, Database Alerts, and database logging.

Complete the form as shown and click the **Connect and Execute Query** button to run the connection test.

Database Connection URL

Enter the connection URL to the database you want to connect to, for example: jdbc:odbc:orders.

Database Driver

Enter the JDBC or ODBC driver that SiteScope should use. The file, .jar file, or library containing the .class file must be installed in the **<SiteScope install path>\SiteScope\java\lib\ext** directory. SiteScope includes with the jdbc/odbc driver used in the example above. To use another driver, you must install the driver file(s) into the proper directory before SiteScope can use them.

Database User Name

Enter the username required to connect to the database.

Database Password:

Enter the password required to connect to the database.

Query

Enter an optional SQL Query to execute on the database. If you do not supply an SQL query string, the loading of the driver and connection to the database will be tested but no query will be executed.

Results Set Max Columns

If you have entered an SQL Query, enter the maximum number of columns to display in the query result set.

Results Set Max Rows

If you have entered an SQL Query, enter the maximum number of rows to display in the query result set.

The following is an example of the data returned from a successful database connection with a SQL query (limited to one row).

server Name	groupID	frame Index	frameI D	setting Name	setting Line	lineChunk	chunk Value
10.0.0.157	master.config	1	_config	_databaseMaxSummary	1	1	200

DNS Lookup

DNS Lookup is a tool which looks up names from a Domain Name Server. It shows you the IP address for a domain name. It also shows you information about the name servers for a domain. When there is a problem on the network, one cause is that the DNS server is not providing the right IP addresses for your servers. You can use this utility to verify that your DNS server is returning the correct addresses for your own servers. You can also use it to verify that it is able to lookup the addresses for external domains.

The DNS Lookup form provides a gateway to the standard nslookup program. It will send the request to the DNS server entered in the “DNS Address” text box. Alternately, it will display the IP address for the host name entered in the "Host Name" text box. Clicking the **DNS Lookup** button initiates the test. The results of the DNS lookup are displayed in the lower portion of the page.

Event Log

The Windows NT Event Log tool displays event log entries on a server. By default the Event Log tool displays entries from the System log for the server on which SiteScope is installed. The log entries are displayed on the lower portion of the Event Log page below the **Show Event Log Entries** button. You can view the entries in the event logs on another server by entering the name of that server in the **Server Name** text box. You use the drop-down list in the **Event Log** box to choose which type of log file to view. The choices include the following:

- System
- Application
- Security

You use the **Entries To Show** box to specify how many entries from the log file you want displayed. The ten most recent entries are shown by default with the latest entry always displayed at the bottom of the list.

Clicking the **Show Event Log Entries** button completes the action and refreshes the log entry listing.

FTP Server

You can use the Check FTP Server tool to access an FTP server and view the interaction between SiteScope (acting as an FTP client) and the FTP server. For example, if you receive an alert from SiteScope indicating that your FTP server is not working properly, the first step is to use this tool to help track down the problem.

To check an FTP server Complete the items on the Check FTP Server form as outlined below. When the required items are complete, click the **Check FTP Server** button to initiate the test.

FTP Server

Enter the IP address or the name of the FTP server that you want to test. For example, you could enter either 206.168.191.22 or ftp.thiscompany.com.

File

Enter the file name to retrieve in this box, for example /pub/docs/mydoc.txt.

User Name

Enter the name used to log into the FTP server in this box.

Password

Enter the password used to log into the FTP server in this box.

Use Passive

Select this box to have SiteScope use a passive FTP connection. This is commonly required to access FTP servers through a firewall.

Proxy

Enter the proxy name or IP address if you want to use a proxy server for the FTP test.

Proxy User Name

Enter the name used to log into the proxy server in this box.

Proxy User Password

Enter the password used to log into the proxy server in this box.

The following is an sample output from the Check FTP Server tool. In this case, the FTP server allowed us to log on without a problem, indicating that the server is running and accepting requests. The failure is caused when the server was unable to locate the file that was requested: file.txt. Correcting this particular problem may be as easy as replacing the missing file or verifying the file location.

```
Received: 220 public Microsoft FTP Service (Version 2.0).
Sent:     USER anonymous
Received: 331 Anonymous access allowed, send identity (e-mail name) as
password.
```

```
Sent:     PASS anonymous
Received: 230 Anonymous user logged in.
Sent:     PASV
Received: 227 Entering Passive Mode (206,168,191,1,5,183).
Connecting to server 206.168.191.1 port 1463
Sent:     RETR file.txt
Received: 550 file.txt: The system cannot find the file specified.
Sent:     QUIT
Received: 221
```

Get URL and URL Content

Use the Get URL and URL Content tool to retrieve an item from a Web server. The URL specifies the server to contact and the item to return. Because SiteScope displays the content of the requested URL, this tool also functions to check URL Content. You can use this utility to verify that a given URL can be accessed from a Web server. You can also use it to see how long it takes for the page to be returned.

Complete the Get URL form as indicated. Clicking the **Get URL** button will initiate the test. The results of the test are displayed on the lower portion of the page. The results include statistics on the URL retrieval as well as a text representation of the URL content.

URL

Enter the URL that you want to test (for example, http://demo.thiscompany.com).

User Name

If the URL specified above requires a name and password for access, enter the user name in this box.

Password

If the URL specified requires a name and password for access, enter the password in this box.

Proxy

Optionally, a proxy server can be used to access the URL. Enter the address or domain name and port of an HTTP Proxy Server.

Proxy User Name

If the proxy server requires a name and password to access the URL, enter the name here.

Proxy Password

If the proxy server requires a name and password to access the URL, enter the password here.

Content Match

Enter a string of text to check for in the returned page or frameset. If the text is not contained in the page, the content match will fail. The search is case sensitive. Remember that HTML tags are part of a text document, so include the HTML tags if they are part of the text you are searching for (for example, "< B> Hello< /B> World").

Error Content Match

Enter a string of text to check for in the returned page or frameset. If the text **is** contained in the page, the test will indicate an error condition. The search is case sensitive.

Retrieve Frames

Check this option to have SiteScope retrieve image data linked to the URL being requested.

Retrieve Images

Check this option to have SiteScope retrieve image data linked to the URL being requested.

LDAP Authentication Test

The SiteScope LDAP Authentication Test verifies that a Lightweight Directory Access Protocol (LDAP) server can authenticate a user by performing a "simple" authentication.

Complete the items on the LDAP Authentication Test form as follows. When the required items are complete, click the **Authenticate User** button.

Security Principal

Enter the constant that holds the name of the environment property for specifying the identity of the principal for authenticating the caller to the service. The format of the principal depends on the authentication scheme. If this property is unspecified, the behavior is determined by the service provider. This should be of the form (uid=testuser,ou=TEST,o=mydomain.com)

Security Credential

Enter the constant that holds the name of the environment property for specifying the credentials of the principal for authenticating the caller to the service. The value of the property depends on the authentication scheme. For example, it could be a hashed password, clear-text password, key, certificate, and so on. If this property is unspecified, the behavior is determined by the service provider.

URL Provider Address

Enter the constant that holds the name of the environment property for specifying configuration information for the service provider to use. The value of the property should contain a URL string (for example, "ldap://somehost:389"). This property may be specified in the environment, an applet parameter, a system property, or a resource file. If it is not specified in any of these sources, the default configuration is determined by the service provider.

LDAP Query

Use this box to enter an object query to look at a LDAP object other than the default user **dn** object. For example, enter the mail object to check for an e-mail address associated with the dn object entered above. You must enter a valid object query in this text box if you are using a LDAP filter (see the description below).

Search Filter

Enter an search filter in this text box in order to perform a search using a filter criteria. The LDAP filter syntax is a logical expression in prefix notation meaning that logical operator appears before its arguments. For example, the item sn=Freddie means that the **sn** attribute must exist with the attribute value equal to Freddie. Multiple items can be included in the filter string by enclosing them in parentheses, such as (sn=Freddie) and combined using logical operators such as the & (the conjunction operator) to create logical expressions. For example the filter syntax (& (sn=Freddie) (mail=*)) requests LDAP entries that have both a sn attribute of Freddie and a mail attribute. More information about LDAP filter syntax can be found at http://www.ietf.org/rfc/rfc2254.txt and also at http://java.sun.com/products/jndi/tutorial/basics/directory/filter.html

Mail Round Trip Test

The SiteScope Mail Test checks a Mail Server via the network. It verifies that the mail server is accepting requests, and also verifies that a message can be sent and retrieved. It does this by sending a standard mail message using SMTP and then retrieving that same message via a POP user account. Each message that SiteScope sends includes a unique key which it checks for to insure that it does not retrieve the wrong message and return a false OK reading.

Complete the items on the Mail Monitor form as follows. When all the fields are complete, click the **Check Mail Server**" button.

Outgoing Mail Server (SMTP)

Enter the hostname of the SMTP mail server to which the test mail message should be sent. (for example, mail.thiscompany.com).

Incoming Mail Server (POP)

Enter the hostname of the POP mail server that should receive the test message. This can be the same mail server to which the test message was sent (for example, mail.thiscompany.com).

Mail Server User Name

Enter a POP user account name. A test e-mail message will be sent to this account and the Mail monitor will login to the account and verify that the message was received. No other mail in the account will be touched; therefore you can use your own personal mail account or another existing account for this purpose.

Note: If you use a mail reader that automatically retrieves and deletes messages from the server, there is a chance that the Mail Monitor will never see the mail message and will therefore report an error.

Mail Server Password

Enter a password, if necessary, for the test mail account.

To Address

Enter the mail address to which the test message should be sent. This should be the address for the POP account that you specified in the **Mail Server User Name** box. For example, if you specified support as the Mail Server User Name, the To Address might be sysadmin@mycompany.com.

Timeout

The number of seconds that the Mail monitor should wait for a mail message to be received before timing-out.

Retrieve Pause

After SiteScope sends the test message, it immediately logs into the mail account to verify that the message has been received. If the message hasn't been received, SiteScope will automatically wait 10 seconds before it checks again. You can adjust this wait time by indicating an alternate number of seconds to wait in this box.

Network

The Network Tool reports the current network interface statistics and lists the active network connections. This information can be useful to determine the health of you network interface. You can also use this tool to track down problems where network connections are being left open or runaway conditions where more and more connections are being opened without ever being closed.

The Network Tool runs once when it is opened and reports the network information. The data returned by the tool are displayed on the lower portion of the Network Tool page. The information can be updated by clicking on the **Run Network** button.

News Server

You can use the Check News Server as a tool to access a news server and view the NNTP interaction between SiteScope (acting as a news client) and the news server.

To perform a news server check, complete the Check News Server form as indicated. You can optionally specify one or more news groups by entering them into the "News group" box. Separate multiple news group names by commas. If the news server requires a username and password, enter them in the boxes provided. Clicking the **Check News Group** button will initiate the test. The results of the test will be displayed in the lower portion of the page.

Ping

Ping is a tool that sends a packet to another location and back to the sender. It shows you the round-trip time along the path. When there is a problem with the network, ping can tell you if another location can be reached. The Ping Tool will do a ping from the current server to another location. Enter the domain name or IP address of the location you want to ping in the text box.

For example, enter either:

demo.thiscompany.com (this is the host name)
OR
206.168.112.53 (this is the IP address)

You will see something like this displayed on the screen:

```
Pinging 206.168.112.53 with 32 bytes of data:
Reply from 206.168.112.53: bytes=32 time=20ms TTL=59
Reply from 206.168.112.53: bytes=32 time=10ms TTL=59
Reply from 206.168.112.53: bytes=32 time=10ms TTL=59
Reply from 206.168.112.53: bytes=32 time=10ms TTL=59
Reply from 206.168.112.53: bytes=32 time=20ms TTL=59
```

The Ping tool page also contains a link to the Trace Route tool. click the **Trace Route** link below the navigation bar at the top of the page.

NT Performance Counter Test

The NT Performance Counter Test is a tool that you can use to check performance counters on a specific machine in an Windows NT/2000 network. It provides is an interface to the perfex.exe executable supplied as part of SiteScope.

Complete the form as shown and click the **List Objects and Enumerate Counters** button to display the individual NT performance counters and corresponding values for the selected counter object. If there are no counter objects available for this machine, the drop-down list that contains the counter objects will indicate this situation. Information about the problem will be shown along with suggested actions to resolve the problem. This tool can be very useful in troubleshooting remote registry connections needed to read performance counters.

Machine Name

Enter a machine name to list all NT performance counter objects available on that machine. A double slash \\ will be added before to any machine name supplied. If this box is left blank the tool will default to the local machine ("this server").

Admin User Account

Enter the administrative password for the machine you want to query. This is only necessary if you running SiteScope under an account that does NOT have administrative privileges to access performance counters for the domain or workgroup you are trying to connect to. If the test indicates you are required to supply a password it means that the remote machine requires authorization to access the performance counter registry.

Password

Enter the administrative password for the machine you want to query. See the note for the **Admin User Account** above.

Counter Object Name

Use the drop-down list to select the counter(s) to list. This box will display one of three values:

- (Choose a counter object) - indicating you need to choose a counter object from the drop-down list then select the **List Objects and Enumerate Counters** button to display the individual NT performance counters and corresponding values for the selected counter object.
- (NO COUNTER OBJECTS AVAILABLE using this username and password) - indicating that you must supply authorization by providing username and password in order to see the counter objects. The remote machine you are connecting to does not recognize the user that the SiteScope service is currently running as a "VALID user with local admin rights". If you believe you have the correct user name and password, click the **List Objects and Enumerate Counters** button to update the display.
- One of the counter objects available on the machine named in the **Machine Name** box, indicating that a counter selection has already been made. The data for that counter should be displayed in the table in the lower portion of the screen.

If the connection to the selected server is successful, the counter information will displayed in the table on the lower portion of the screen. The table shows the counter name, the value, and a description of the counter provided by the counter registry. The table has the following format:

Counter Name	Counter Value	Counter Description

Other troubleshooting tips are available on the NT Performance Counter Test screen.

Processes

The Processes tool displays processes running on the server where SiteScope is installed. This can be useful to confirm that critical services are available. It is also possible to view services running on another server by entering the name of that server in the **Server Name** text box or selecting a Remote Unix server from the drop down menu. Click the **Show Services** button to initiate the action.

A listing of the services available on the server is displayed on the Services page below the **Show Services** button. At the bottom of this listing is a "Go to **Process Detail** link that you can use to display a listing of the current processes running on the local server or the server specified in the Server Name box. Use the "Got to **Services** link at the bottom of the Process Detail listing to toggle back to the services listing for that server.

Regular Expression Test

Cut and paste a portion of text on which you want to perform a regular expression match into the text box labeled **Your Text that will be matched**. For efficiency in developing regular expressions, you should include all of the content that would precede the target data or pattern that you want to match. For example, when developing a regular expression for content matching on a Web page, you should use the Get URL and URL Content tool to retrieve the entire HTTP content including the HTTP header.

You enter your test regular expression into the field labeled **Your Regular Expression**. For content with multiple lines with carriage returns and line feeds, you should consider adding the s search modifier to the end of the expression to have the content treated as a single line of text. For example, /value:\W[\d]{2,6}/s.

Click the **Test Your Match** button to perform the match test.

The results of the test are displayed in the area below the **Test Your Match** button. If there is a problem with your regular expression, an error message is displayed. If the match was successful the following data is displayed:

Parsed parentheses and matches

This section includes a table that displays any matches requested as retained values or back references by pairs of parentheses inside the regular expression. If your expression does not include parentheses, this table will be empty. The two columns of the parsed parentheses table are:

- **Parentheses counted from left** - this displays any patterns in the regular expression delimited by parentheses as counted from the left hand side of the expression.
- **matching text** - This table cell displays the text that matched the parenthesis marked patterns listed in the column to the left.

Below this table is the **Whole Match Between Slashes** text area. This echoes the entire content entered in the **Your Text that will be matched** field. The content that matched the pattern in your regular expression will be highlighted within this content, normally using a blue color font. This can be very useful to show possible problems with "greedy" expressions that use wildcards like the .* pattern that tend to match too much content. It can also uncover problems of duplicate patterns within the content which require that you add other unique patterns to your expression in order to match the desired portion of the content.

SNMP Browser Tool

The SNMP Browser Tool provides a browsable tree representation of an SNMP agent's MIB. It can be used to verify the connection properties of an SNMP agent and to gain more information about the MIB(s) which that agent implements.

This tool operates by traversing all of the OIDs on a given agent and then using the MIB information in the SiteScope/templates.mib directory to build a tree-structured XML representation of the OIDs. Included in the XML tree are the textual and numeric names of the OIDs, their descriptions (if available), and their values at the time of traversal.

The XML is displayed in a separate browser window, using the browser's default display for XML data. For IE and Netscape/Mozilla browsers, this default display is in the form of a collapsible, hierarchical tree. If errors occur during the MIB traversal, then an error message describing the problem is printed in the new window (instead of XML).

The SNMP by MIB Tool is intended to help in configuring any of the SNMP-based monitors, including:

- SNMP by MIB Monitor
- SNMP Monitor
- Cisco Works Monitor
- F5 SNMP Monitor

Complete the tool form as shown and click the **Browse** button to open a new window containing a browsable view of the MIB (in XML).

Host or IP Address

Enter the hostname or IP address of the device on which the SNMP agent is running.

Port

Enter the port on which the SNMP agent is listening. This is usually 161, which is also the default.

MIB

Choose the MIB which you would like to view. If you select "All MIBs", then all data obtained during the MIB traversal will be displayed. If you select a specific MIB, then only the OIDs within that MIB will be displayed. This list of MIBs can be updated or extended by placing new MIB files in the SiteScope/templates.mib directory.

Version

Select the version of SNMP which the tool should use when connecting to the agent.

V1/V2 Community

For version 1 or 2 connections, enter the community string to use when connecting to the SNMP agent.

V3 Authentication Type

Select the type of authentication to use for a version 3 connection.

V3 Username

Enter the username for a version 3 connection.

V3 Authentication Password

Enter the password to use for authentication in a version 3 connection.

V3 Privacy Password

Enter the password to use for DES privacy encryption in a version 3 connection. Leave this field blank if no privacy is desired.

V3 Context Engine ID

Enter a hexidecimal string representing the Context Engine ID to use for this connection. This is applicable for SNMP V3 only.

V3 Context Name

Enter the Context Name to use for this connection. This is applicable for SNMP V3 only.

SNMP

The SNMP tool lets you query a SNMP Management Information Base (MIB) and retrieve a set of OIDs.

Fill out the SNMP tool form as shown below then click the **Next Block of OIDs** button to perform the query (GET).

Host IP Address

Enter the IP Address of the server that hosts the SNMP MIB you want to query. By default, this will connect to port 161. If your SNMP device is using a different port, add it to the hostname using ":port". For example, to use port 170, you would enter demo.sitescope.com:170.

Next OID

Enter the OID of the next OID that should be retrieved.

Index

Enter the index of the SNMP object. Values for an OID come as either scalar or indexed (array) values. For a scalar OID, the index value must be set to 0. For an indexed value, you must provide the index (a positive integer starting with 1) to the element that contains the value you want. For example, the OID 1.3.6.1.2.1.2.2.1.17 is an indexed value that contains four elements. To access this second element of this OID you enter an index of 2 in this text box.

Community

Enter the Community string for the SNMP device. Most devices use "public" as a community string. If the device you are testing requires a different Community string, supply it in this box.

Version (V1 or V2)

Select the SNMP version used by the SNMP host you want to test. SiteScope supports both SNMP version 1 and version 2.

Number of Records to get

Enter the number of OID record to retrieve.

The SNMP OID's returned by the SNMP Tool are displayed in the lower portion of the screen.

SNMP Trap

The SNMP Trap log tool lets you view SNMP Trap received by SiteScope's SNMP listener. The tool is only enabled if you have already created one or more SNMP Trap Monitors. Creating an SNMP Trap Monitor will enable the SiteScope SNMP Trap Log. A message at the top of the tool page will indicate **Receiving SNMP Traps is not active** if the SNMP Trap Log is not currently active.

Fill out the SNMP Trap log tool form as shown below then click the **Show SNMP Trap Log Entries** to view the log based on the search criteria you have entered.

Traps To Show

Enter the number of SNMP Traps to list. The default is 10. The most recent SNMP Traps received by SiteScope are displayed first.

Content Match

Enter an optional text string or regular expression to be used to match entries in the SNMP Trap Log. Content matching can be done for data from any of the columns of the log such as OID, Community, Agent, and so forth (see the SNMP Trap Log table format below).

The SNMP traps in the SiteScope SNMP Trap Log are displayed in the SNMP Trap Log table. The number of traps matching the search criteria are displayed in the table title. The format of the table is as follows:

SNMP Trap Log (0 traps)

Date	From	Message	Trap	Specific	OID	Agent	Community	Trap Time

Services

The Services tool displays NT services running on the server where SiteScope is installed. This can be useful to confirm that critical services are available. It is also possible to view services running on another server by entering the name of that server in the **Server Name** text box. Click the **Show Services** button to initiate the action.

A listing of the services available on the server is displayed on the Services page below the **Show Services** button. At the bottom of this listing is a "Got to **Process Detail** link that you can use to display a listing of the current processes running on the local server or the server specified in the Server Name box. Use the "Got to **Services** link at the bottom of the Process Detail listing to toggle back to the services listing for that server.

Trace Route

Trace Route is a tool that shows you the network path between two locations. It shows you the address and how long it takes to get to each hop in the path. When there is a problem with the network, traceroute can often be used to narrow down where the problem is occurring. This tool will do a traceroute from your server to another location. The Trace Route tool is accessible by a link below the navigation bar on the Ping, the Get URL, and DNS Lookup tool pages.

The Trace Route form provides a gateway to the standard traceroute program which determines the route across a network taken by packets from one host to another host. In this case, the traceroute will start from your server. It will display the path taken to reach the host or IP address you have listed in the text box.

You can use this utility to verify connectivity of a host and determine how the host is connected to the Internet. You can also determine the path taken from your server to the specified host. This will allow you, for example, to determine where packet loss may be occurring when you attempt to connect to hosts elsewhere on the Internet.

To perform a traceroute, enter the domain name or IP address of the other location in the text box. Clicking the **Trace Route** button initiates the action.

Note: For the Unix version of SiteScope you must specify the pathname to the traceroute utility on the server that SiteScope is running on.

To do this you must:

1 Stop the SiteScope process.

2 Edit the **<SiteScope install path>/SiteScope/groups/master.config** file to add the path to the traceroute utility to the _tracerouteCommand= property entry (for example: _tracerouteCommand=/usr/sbin/traceroute).

3 Save the change to the master.config file.

4 Restart the SiteScope process.

Check URL Sequence

The Check URL Sequence Tool simulates a user's session across several pages. An example of this would be entering an account name via a Web form, checking an account status for the page that is returned, and then following a sequence of links through several more pages. The Check URL Sequence Tool page is accessed either by clicking on the **Tools** link that is displayed with the monitor status in the Monitor Detail table or by clicking on the Check URL Sequence link on the Diagnostic Tools page.

Note: Accessing the Check URL Sequence Tool via the Monitor Detail page is considered to be more useful than using it as a diagnostic tool. Access via the Monitor Detail page allows you to modify existing URL Sequences including use of the URL Sequence Wizard.

A URL Sequence is specified by giving a URL to start at and then specifying either additional URL's, or more commonly, links or buttons to follow. For each step you may specify a match or error string to search for, a user name and password to enter, and POST data for that step.

The URL Sequence tool returns the status and time taken for each step in the sequence. It also embeds a copy of the page returned at each step of the sequence in it is output so that a more graphical view of the sequence can be viewed. Note that any graphics referenced by these pages will show up as broken - this is so that the HTML that is output is the exact same HTML that was retrieved, making debugging more precise.

Complete the items on the Check URL Sequence form as follows. When the required items are complete, click the **Check URL Sequence** button to test the transaction or the **Update Monitor** button to save any changes that you have made to the current monitor. Press the Press the **Wizard** button to edit the existing sequence in the URL Sequence Wizard interface.

Step 1 - Reference

Select the type of object or target from the drop-down list in the first column. This represents the either a Web page, a hyper link, form element, and so forth, that defines the sequence path. The type for Step 1 should always be a URL. Enter the specific URL of the first page in the sequence that you want SiteScope to complete. For example, if you want SiteScope to test your order process, you might enter a URL such as
https://www.securecompany.com/order.html

Step (2 thru N) - Reference

From Step 2 on, you must tell SiteScope what you want it to do next. In the Type column, tell SiteScope what type of item it will be looking for in this step. For example, if SiteScope will be doing the equivalent of selecting a submit button, you would choose the **Form - match the displayed name of a Submit button**. SiteScope uses this information to scan the HTML for the proper text matches.

Enter the URL, link, or submit button to be followed in the second column for this step. For example, if SiteScope should follow the submit button on the page and the name on the button (its value) is "Place My Order", type Place My Order in this box. To instruct SiteScope to follow a link on the page, type the text of the link. For example, if the link says **Next**, type the word Next in this box. You can also type in a full URL.

If an image is used as the submit button, you must enter the name value for the image. You will find this by looking at the HTML for the form.

The Advanced Settings section gives you the ability to customize error and warning thresholds, or complete other optional settings.

POST Data

If this step contains a URL for a POST request, enter the post variables, one per line as name=value pairs. This option is used to verify that a form is working correctly by performing the same request that occurs when a user submits a form. See also the Match Content box for a way to verify that the correct form response was received. If this item is blank, a GET request is performed.

Match Content

Enter an expression describing the values to match in the returned page. If the expression is not contained in the page, the monitor will display "no match on content". A regular expression can be used to define the values to match.

Error If Match

Enter an expression describing the values that, if found on the page returned, indicate an error in the sequence process. For example, if the phrase "Login Error" appears there may be a problem with user profile data. If the Error If Match expression is found in the page, the monitor will signal an error. A regular expression can be used to define the values to match.

User Name

Enter the user name, if any, required for this step.

Password

Enter the password, if any, required for this step.

Delay

Enter an optional delay period that SiteScope will wait before executing the next step.

Title

Enter an optional title to be associated with this step of the sequence. It is best to select a title that describes what is being accomplished in this step.

Web Service

The Web Service Test is used to check Simple Object Access Protocol (SOAP) enabled Web services for availability, stability or if you just need to see what an actual SOAP response looks like. It is also useful for diagnosing a Web service request failure, or for picking out match strings for use with a specific Web Service Monitor. The Web Service Test sends a SOAP request to the server and checks the HTTP response codes to verify that the service is responding. The actual SOAP response is displayed, but no further verification is done on this returned message.

The Simple Object Access Protocol (SOAP) is a way for a program running under one operating system to communicate with another program running under the same or different operating system (such as a Win 2000 program talking to a Linux based program) The Simple Object Access Protocol uses the Hypertext Transfer Protocol (HTTP) and Extensible Markup Language (XML) for information exchange with services in a distributed environment.

Status

The possible status values returned by the test are:

- OK
- unknown host name
- unable to reach server
- unable to connect to server
- timed out reading
- content match error
- document moved
- unauthorized
- forbidden
- not found
- proxy authentication required
- server error
- not implemented

➤ server busy

Support Levels

The following specification features are currently supported:

➤ WSDL 1.2

➤ SOAP 1.1

➤ Simple and Complex Types based on XML Schema 2001

➤ SOAP binding with the HTTP(s) protocol only

➤ SOAP with Attachments is not supported

Be advised that SOAP and WSDL technologies are still undergoing evolution. Consequently there can be instances of WSDL documents that SiteScope may not be able to process with complete accuracy. In addition, certain SOAP requests that SiteScope sends may not interact effectively with all Web service providers due to inherent specification ambiguities. However, it is our full intent and commitment to continually keep monitor implementations up to date with the latest Web service specifications.

Tip: A quick way to fill out this form is to first create a Web service monitor for the service you need to test. There in the "Add Web Service Monitor" page, you merely need to specify the WSDL file of the target Web service. SiteScope will parse the WSDL file and present a list of methods to choose from. It will then generate a skeleton parameter list for your selected method, for you to flesh out actual parameter values. Save and create this Web service, which causes SiteScope to send the proper SOAP message to invoke the service method (that may or may not succeed). But once the Web service monitor is created, it should now be listed in your Group monitors display page. Click the "Tools" link for this Web service monitor and you are back in the "Test Web Service" page but this time with the test form filled out properly and sufficiently.

Otherwise, manually complete the items on the Add Web Service Test form as follows. When the required items are complete, click the **Web Service Request** button.

WSDL Path or URL

Enter the URL or the file path of the WSDL file to be used for this monitor. If a WSDL file path is specified it must be relative to **<SiteScope install path>/SiteScope/templates.wsdl/**, where *ssHome* is where SiteScope was installed on your system. In addition, your WSDL files must have an extension of *.wsdl*.

Web Service URL

Enter the URL of the Web service to be tested.

Method Name

Enter the name of the method to be invoked.

Arguments

Enter the arguments to the method specified above and their types. Specify simple type parameters in the form:

parm-name(*parm-type*) = *value*

where the parameter names and types must match the service method specifications of its WSDL file exactly. The *value* must of course agree with the parameter data type otherwise the request will fail. Strings with embedded spaces should be enclosed in double quotes. Each parameter must be in a separate line, i.e. you must add a carriage return at the end of each parameter value, as shown in the example parameter list below:

```
stockSymbol (string) = MERQ
numShares (int) = 10
```

A complex type parameter must be represented as one long string. An example of a complex type parameter is shown below (line breaks are for readability purposes only):

```
stocksymbol[COMPLEX] =<stocksymbol
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:fw100="urn:ws-stock"
xsi:type="fw100:getQuote"> <ticker
xsi:type="xsd:string">MERQ</ticker></stocksymbol>
```

SiteScope does not perform any validation on your input parameter lists, so make sure your complex type values are valid and well-formed XML strings. Do not add any carriage returns within a complex type parameter - only at the end.

If the Web service method does not take any parameters, the text box should be left empty.

SOAP Action URI

The SOAP Action URI in the header of the SOAP request to the Web Service. During initial setup this will be extracted from the WSDL file.

Method Namespace

The XML name space for the method in the SOAP request. During initial setup this value will be extracted from the WSDL file.

User Name

If the URL specified requires a name and password for access, enter the name in this box.

Password

If the URL specified requires a name and password for access, enter the password in this box.

Proxy

Optionally, a proxy server can be used to access the URL. Enter the domain name and port of the HTTP Proxy Server.

XML Transform Test

Use this tool to test a user defined XSL file that can be used to transform an XML file or output. This might be a file from a Web application which contains performance metrics data. The use of an XSL transform may be necessary to process the XML data into an acceptable format for use by the Browsable XML Monitor type. The format rules for said input XML are:

XML URL

Enter the URL of the XML file that will be the input for the transformation.

XSL File

Enter the path to the XSL file you want to test.

User Name

If access to the target XML file requires authentication, enter the username needed to access the content in this field.

Password

If access to the target XML file requires authentication, enter the password needed to access the content in this field.

Proxy

If you are using a proxy in order to access the target XML content, enter the address of the proxy in this field.

Proxy User Name

If you are using a proxy in order to access the target XML content, enter the username needed to use the proxy in this field.

Proxy Password

When using a proxy in order to access the target XML content, enter the password needed to use the proxy in this field.

TEC Event History

TEC Event History tool is used for working with the Tivoli Alert Monitor This tool lets you view recent TEC events received by the TEC event listener included with SiteScope and make adjustments in the EMS Configuration file for the Tivoli Alert Monitor.

Note: This tool is only enabled if you have a valid EMS monitor license in the **Option Licenses** box on the General Preferences page and integration with other, applicable Mercury products.

To view recent TEC events, complete the TEC Event History tool form as shown below then click the **Show TEC Event History Entries** to view the events.

Set History Capacity

Select the number of TEC events to store in the History. The default is 20. The most recent TEC events received by SiteScope are displayed first.

The TEC events in the SiteScope TEC Event History are displayed in the TEC Event History table. The number of event stored in the history displayed in the table title. The format of the table is as follows:

TEC Event History (0 events)

Date	Class	Message	Severity	Status	Source	Host name	Message

To view all event details for particular event click the Class field for the event. Details are shown in the separate window.

Index

A

Active Directory
  monitoring solution 85
Active Directory Replication Monitor 895
  advanced settings 897
  editing 896
Active Directory solution template
  deploying 87
  settings 88
Apache Server Monitor 143
  advanced settings 145
  configuring 144
ASP Server Monitor 151
  advanced settings 154
  configuring 152
Avalon Event Monitor 1069
  setup requirements 1070

B

BMC Patrol Event Monitor 1079
  PTI installation and configuration 1084
BMC Patrol Metrics Monitor 1097
  diagnostics 1098
  system requirements 1098
BroadVision Application Server Monitor 159
  advanced settings 162
  configuring 160
Browsable Windows Performance Counter Monitor 1033
  advanced settings 1035
  editing 1034

C

CA Unicenter Event Monitor 1109
  about 1109
  CA Integration Add-on log file 1115
  installation of CA Integration module 1112
Check FTP Server diagnostic tool 1336
Check News Server tool 1343
Check Point Firewall-1 Monitor 167
  advanced settings 169
  configuring 167
Check URL Sequence Tool 1353
CIM Monitor 1123
Cisco Works Monitor 175
  advanced settings 181
  configuring 175
Citrix Server Monitor 187
  configuring 188
  troubleshooting tips 195
ColdFusion Server Monitor 205, 681
  advanced settings 208, 689
  configuring 206, 682
COM+ Server Monitor 903
  advanced settings 907
  configuring 905
  main settings 905
  probe installation 904
Compaq Insight Manager Event Monitor 1123
  about 1123
  setup requirements 1124
Composite Monitor 197
  advanced settings 199
  configuring 198
Concord Metrics Monitor 1135
  about 1135
  setup requirements 1136
configuration file templates 1059
CPU Utilization Monitor 213

advanced settings 215
configuring 214

D

Database Counter Monitor 221
advanced settings 226
editing 223
Database Query Monitor 233
advanced settings 237
configuring 235
notes on monitoring common databases 243
setup requirements for 234
databases
monitoring 243
DB2 8.x Monitor 261
advanced settings 266
configuring 262
DB2 Monitor 249
advanced settings 255
configuring 250
DHCP Monitor 289
advanced settings 291
configuring 290
installation of DHCP software library 290
diagnostic tools 1331
Check FTP Server 1336
Check News Server 1343
Check URL Sequence Tool 1353
DNS Lookup 1335
Get URL and URL Content Tool 1338
LDAP Authentication Test 1339
Mail Round Trip Test 1341
Network Tool 1343
NT Event Log tool 1336
NT Performance Counter Test 1344
Ping 1343
SNMP 1349
SNMP Trap 1351
TEC Event History tool 1360
TraceRoute 1352
Web Service Test 1356
Directory Monitor 281
advanced settings 283
configuring 282
Disk Space Monitor 273
advanced settings 275
configuring 274
DNS Lookup diagnostic tool 1335
DNS Monitor 297
advanced settings 299
configuring 298
Dynamo Application Server Monitor 305
advanced settings 308
configuring 306

E

eBusiness Chain Monitor 315
advanced settings 319
configuring 318
passing values between monitors 324
setting up monitors for 317
Exchange
monitoring solution 91
Exchange 2000/2003 Message Traffic Monitor 929
advanced settings 932
editing 930
Exchange 2003 Mailbox Monitor 913
advanced settings 915
editing 914
Exchange 2003 Public Folder Monitor 921
advanced settings 923
editing 922
Exchange 5.5 Message Traffic Monitor 937
advanced settings 939
editing 938
Exchange solution template
deploying 94, 100
settings 95

F

F5 Big-IP Monitor 325
advanced settings 328
configuring 325
File Monitor 335
advanced settings 338
configuring 336

Formula Composite Monitor 345
advanced settings 348
configuring 347
FTP Monitor 355
advanced settings 358
configuring 357

G

Get URL and URL Content Tool 1338
groups
in templates 51

H

HP OVO Event Monitor 1147, 1161
about 1147, 1161
Add-on installation instructions 1150
configuring the Integration Add-on 1151
starting and stopping the HP OVO Integration Add-on 1152
HP OVO Integration Installation 1149

I

IIS Server Monitor 365
advanced settings 368
configuring 366
integration
with SNMP management systems 629
Integration Monitor logging options 1046
Integration Monitor troubleshooting 1047
Integration Monitors xvii
configuration file templates 1059
configuration files 1049
configuration files, action directive 1056
configuration files, conditional expressions 1056
configuration files, configuring event template 1060
configuration files, configuring the metrics template 1065
configuration files, event handler structure 1052
configuration files, example event file 1064
configuration files, example metrics template 1066
configuration files, examples 1058
configuration files, introduction 1049
configuration files, matching condition 1052
configuration files, string expressions 1056
configuration files, structure 1051
configuration files, tags 1057
working with 1043
iPlanet Server Monitor 373, 387
advanced settings 381
configuring 375

J

JavaScript in URL sequences 740
JMX Monitor 395
advanced settings 398
configuring 397

L

LDAP Authentication Test 1339
LDAP Monitor 403
advanced settings 406
configuring 404
Link Check Monitor 413
advanced settings 416
configuring 414
Log File Monitor
advanced settings 428
configuring 424
monitors
for checking log files 423
logging
Integration Monitors, options 1046

M

Mail Monitor 435
advanced settings 438
configuring 436
Mail Round Trip Test diagnostic tool 1341
MAPI Monitor 445

advanced settings 450
configuring 449
Memory Monitor 455
advanced settings 458
configuring 457
Mercury Application Mapping Monitor 1173
monitor
creating using templates 43
monitor templates 43
monitor types 16
ports used 21
Monitor What Matters wizard 69
categories 75
infrastructure settings 75
template reference 75
monitoring
deployment using templates 43
DHCP 289
disk space 273
file systems 281
MQ events 1022
monitoring CIs
Monitor What Matters wizard 69
monitoring remote servers 19
monitors
adding to group 4, 25
by categories 18
classes of SiteScope 16
deleting 27
deleting groups 6
editing 26
editing groups 5
for Active Directory 85
for business processes 315
for checking event logs 835
for checking hyperlinks 413
for checking script execution 573
for combining metrics 345
for CPU utilization 213
for databases 233
for file transfers 355
for files 335
for matching content on Web pages 713
for media files 553
for memory usage 455
for Microsoft Exchange 91
for NNTP 485
for Oracle databases 97
for performing database queries 233
for services and processes 587
for Siebel servers 115
for Web page monitoring 695
for Weblogic servers 127
for WebSphere servers 135
for Windows counters 845
for XML data 881

N

Netcool Event Monitor 1185
about 1185
Setup Requirements 1186
NetIQ Metrics Monitor 1195
about 1195
Network Bandwidth Monitor 463
advanced settings 466
configuring 464
Network Monitor 477
configuring 478
Network Node Manager
forwarding events from 1325
writing scripts to export data 1326
Network Node Manager Integration
about 1325
Network Tool 1343
News Monitor 485
advanced settings 488
configuring 486
NT Event Log tool 1336
NT Performance Counter Test 1344

O

Oracle
monitoring solution 97
Oracle Database Monitor 503
configuring 505
Oracle Database solution template
deploying 99
settings 101
template tools for 103

Oracle9i Application Server Monitor 493
advanced settings 496
configuring 494

P

Ping diagnostic tool 1343
Ping Monitor 513
advanced settings 515
configuring 514
Port Monitor 521
advanced settings 523
configuring 522

R

Radius Monitor 529
advanced settings 531
configuring 530
Real Media Player Monitor 537
advanced settings 540
configuring 538
Real Media Server Monitor 545
advanced settings 548
configuring 546
Real Time Streaming Protocol Monitor 553
regular expressions
in template monitors 62
Remedy Add-on
configuring 1211
Remedy Ticketing Monitor 1207
about 1208
forwarding ticket information to Application Management 1214
HelpDesk integration options for SiteScope 1211
Remedy terminology 1207
software requirements 1209
RTSP Monitor 553
about 553
advanced settings 558
configuring 557

S

SAP
monitoring solution 107
SAP CCMS Alerts Monitor 955
software requirements 956
user authorization settings 947, 956
SAP CCMS Monitor 945
Java connector installation 949
SAP J2EE solution template 111
SAP Java Web Application Server Monitor 967
SAP Monitor 563
advanced settings 568
configuring 565
SAP R/3 solution template 108
settings 110
system requirements 108
SAP Work Processes Monitor 975
Script Monitor 573
advanced settings 578
configuring 576
script return status example 583
setting a timeout value for script execution 584
Service Monitor 587
advanced settings 589
configuring 588
Show Page button 740
Show Source button 740
Siebel
monitoring solution 115
Siebel Application Server Monitor 995
advanced settings 1000
configuring 998
system requirements 995
Siebel Application Server Solution 116
deploying 117
settings 119
system requirements 117
Siebel Gateway Server Solution 122
deploying 122
settings 123
Siebel Log File Monitor 985
advanced settings 989
configuring 986
Siebel Server Manager Monitor 995
Siebel Web Server Monitor 1007
advanced settings 1013
configuring 1008

Siebel Web Server Solution 124
deploying 124
settings 125
system requirements 124
SilverStream Server Monitor 595
about 595
advanced settings 598
configuring 596
sis_configtemplate 43
sis_templatealert 45
sis_templategroup 45
SiteScope
creating templates 48
monitor types 16
Monitor What Matters wizard 69
solution templates 81
SiteScope groups
working with 3
SiteScope monitoring
ports used for 21
remote servers 19
SiteScope Monitors xvii, xviii
SiteScope monitors
working with 15
SNMP by MIB Monitor 617
advanced settings 621
configuring 618
troubleshooting MIB compilation 626
SNMP diagnostic tool 1349
SNMP Monitor 605
advanced settings 609
configuring 606
SNMP Trap diagnostic tool 1351
SNMP Trap Monitor 629
advanced settings 632
configuring 630
solution templates
for Active Directory 85
SAP J2EE 111
SAP monitors 107
SiteScope 81
solutions sets
for BEA WebLogic 127
for IBM WebSphere 135
for Microsoft Exchange 91
for Oracle database 97
for Siebel servers 115
SQL Server Monitor 637
advanced settings 640
configuring 638
SunONE Server Monitor 645
advanced settings 648
configuring 646
supported counters 653
Sybase Monitor 659
advanced settings 665
configuring 660

T

TEC Event History tool 1360
Technology Database Integration Monitor 1223, 1279
setup requirements 1225, 1281
step-by-step integration guide 1237
troubleshooting 1240, 1289
Technology Log File Integration Monitor 1243
setup requirements 1244
step-by-step integration guide 1256
troubleshooting 1259
Technology SNMP Trap Integration Monitor 1261
about 1261
configuring 1264
setup requirements 1262
step-by-step integration guide 1272
troubleshooting 1274
verify SNMP trap reception 1275
template
add regular expression matching 64
adding alerts 52
adding browsable counter monitors 60
adding groups 51
adding monitors 52
applying 65
configuring 50
copying configurations into 50
counter selection examples 63
counter selection using regular expressions 62

creating 48
creating containers 48
creating manually 51
creating variables 57
deploying monitoring 65
exporting 67
importing 67
monitor counter selection in 60
objects 45
planning 47
referencing variables example 59
referencing variables in 58
SERVER_LIST variable 56
system variables 56
to import or export 66
understanding 45
user-defined variables 54
variable syntax 54
variables 53
templates 43
Thresholds Settings
SAP CCMS Alerts monitor 963
Tivoli DM Metrics Monitor 1291
about 1291
configuring 1293
configuring Tivoli environment 1292
Tivoli TEC Event Monitor 1301
about 1301
configuring 1304
TraceRoute diagnostic tool 1352
troubleshooting
a monitored system 1331
Integration Monitors 1047
monitor configuration 1331
Tuxedo Monitor 671
advanced settings 675
configuring 672

U

URL Content Monitor 713
advanced settings 716
Application Management settings 722
configuring 715
URL List Monitor 725
advanced settings 728
configuring 727
URL Monitor 695
advanced settings 699
configuring 698
URL Sequence Monitor 735
beginning a new 739
copying HTML source in steps 740
defining the next step 739
following a META REFRESH 744
go to another URL manually 741
limitations on embedded scripts 740
retaining and passing values between steps 759
selecting a Frame 743
selecting a hyperlink 741
setting status thresholds 756
tools for viewing step content 740
viewing steps in a browser 740

V

variables
creating for templates 57
in templates 53

W

Web Server Monitor 761
advanced settings 763
configuring 762
Web Service Monitor 769
advanced settings 773
configuring 771
Web Service Test 1356
WebLogic
monitoring solution 127
WebLogic Application Server Monitor 781
advanced settings 788
configuring 784
WebLogic solution template
deploying 130
selecting modules to monitor 133
settings 131
using 129
WebSphere
monitoring solution 135

WebSphere Application Server Monitor 793
advanced settings 801
configuring 798
WebSphere MQ Status Monitor 1019
advanced settings 1026
authentication 1024
configuring 1024
main settings 1025
selecting measurements 1026
WebSphere Performance Servlet Monitor 807
advanced settings 810
configuring 808
WebSphere solution template
deploying 138
settings 139
system requirements 138
using 137
WhatsUp Event Monitor 1313
about 1313
configuring 1314
Windows Dial-up Monitor 825
advanced settings 828
configuring 827
Windows Event Log Monitor 835
advanced settings 838
configuring 836
Windows Media Player Monitor 855
advanced settings 858
configuring 856
Windows Media Server Monitor 863
advanced settings 866
configuring 864
Windows Performance Counter Monitor 845
advanced settings 847
configuring 845
main settings 846
Windows Resources Monitor 817, 871
about 817
advanced settings 819, 875
configuring 818, 872

X

XML Metrics Monitor 881
configuring 882