

SECURESPHERE®

Administration Guide

Version 9.5

July 2012

www.imperva.com

COPYRIGHT NOTICE

© 2002 - 2012 Imperva, Inc. All Rights Reserved.

This document is for informational purposes only. Imperva, Inc. makes no warranties, expressed or implied.

No part of this document may be used, disclosed, reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of Imperva, Inc. To obtain this permission, write to the attention of the Imperva Legal Department at: 3400 Bridge Parkway, Suite 200, Redwood Shores, CA 94065.

Information in this document is subject to change without notice and does not represent a commitment on the part of Imperva, Inc. The software described in this document is furnished under a license agreement. The software may be used only in accordance with the terms of this agreement.

This document contains proprietary and confidential information of Imperva, Inc. This document is solely for the use of authorized Imperva customers. The information furnished in this document is believed to be accurate and reliable. However, no responsibility is assumed by Imperva, Inc. for the use of this material.

TRADEMARK ATTRIBUTIONS

Imperva and SecureSphere are trademarks of Imperva, Inc.

All other brand and product names are trademarks or registered trademarks of their respective owners.

Follow this link to see a complete statement of Imperva, Inc.'s copyrights, trademarks and acknowledgements:

https://www.imperva.com/sign_in.asp?retURL=/articles/Reference/SecureSphere-Trademark-Attributions

PATENT INFORMATION

The software described by this document is covered by one or more of the following patents:
US Patent Nos. 7,752,662, 7,743,420, 7,640,235, 8,024,804, 8,051,484, and 8,056,141.

Imperva Contact Information

US Headquarters Imperva Inc. 3400 Bridge Parkway, Suite 200 Redwood Shores, CA 94065 USA Tel: (650) 345 9000 Fax: (650) 345 9004	Email: info@imperva.com Website: www.imperva.com

END USER LICENSE AND SERVICES AGREEMENT

BY CLICKING ON THE "ACCEPT" BUTTON, TAKING AN ACTION TO INDICATE ACCEPTANCE, OR USING THE PRODUCTS (AS DEFINED BELOW) END USER AGREES TO THE TERMS OF THIS END USER LICENSE AND SERVICES AGREEMENT ("AGREEMENT") WITH IMPERVA, INC. ("IMPERVA"). IF END USER DOES NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, CLICK THE "CANCEL" BUTTON, DISCONTINUE THE SET-UP AND INSTALLATION OR DISCONTINUE USE OF THE PRODUCT. IF THE TERMS OF THE AGREEMENT ARE CONSIDERED AN OFFER, ACCEPTANCE IS EXPRESSLY LIMITED TO THESE TERMS. IMPERVA MAY MODIFY OR AMEND THIS AGREEMENT AT ANY TIME AND MAY PROVIDE NOTICE OF SUCH CHANGES BY POSTING A REVISED AGREEMENT AT HTTP://WWW.IMPERVA.COM/OTHER/LICENSE_AGREEMENT.ASP. YOUR CONTINUED USE OF SERVICES WILL CONSTITUTE YOUR ACCEPTANCE OF ANY SUCH CHANGES.

1. Definitions. The following capitalized terms shall have the meanings set forth below:

   a. "Appliance" means the Imperva branded computer hardware on which the Software operates.

   b. "Delivery" shall mean, (i) in the case of Software, when the Software is made available by Imperva for End User to electronically download; (ii) in the case of Services, when the Service has been provisioned and made available to End User to access; and (iii) in the case of an Appliance, when the Appliance has been tendered by Imperva for shipment.

   c. "Documentation" means Imperva's technical specifications that accompany and describe the installation, use and operation of a Product.

   d. "End User" means the party that has purchased the Products for its own use, either directly from Imperva or thru an authorized third party.

   e. "Licensed Volume" means the volume or other measurement of permitted use for the Products as agreed to by Imperva.

   f. "Open Source Software" means third party software that Imperva distributes with the Software pursuant to a license that requires, as a condition of use, modification and/or distribution of such software, that the software or other software combined and/or distributed with it be (i) disclosed or distributed in source code form; (ii) licensed for the purpose of making derivative works; or (iii) redistributable at no charge.

   g. "Product" mean Appliances, Software or Services as the case may be.

   h. "Software" means Imperva's or its licensors' software (in object code format) or content, any updates or upgrades thereto provided to End User by Imperva and any Documentation pertaining thereto. Software may be delivered to End User on Appliances or on a standalone basis. Software does not include any Open Source Software.

   i. "Services" means the subscription services, including content, updates and upgrades thereto, offered by Imperva or that may be made available to End User by Imperva directly or thru its partners and suppliers. Services include, without limitation, the ThreatRadar service and Imperva offered services that are "powered by Incapsula."

   j. "Support and Maintenance" means the technical support services and periodic bug fixes and updates that Imperva may make available to End Users.

   k. "Professional Services" means the installation and configuration services that Imperva may provide to an End User.

2. Licenses and Restrictions.

   a. Software. Subject to the terms and conditions of this Agreement, Imperva grants End User a nonexclusive, nontransferable, nonsublicensable, perpetual license to use the Software only for End User's internal business purposes on the Appliances or in the Licensed Volume purchased by End User. If End User purchases Software on a standalone basis, the license granted herein shall include the right to copy the Software.

   b. Services. Subject to the terms and conditions of this Agreement, Imperva grants End User a nonexclusive, nontransferable, nonsublicensable, revocable license to use and access the Services only for End User's internal business purposes.

   c. Restrictions. End User may not (and may not permit any third party to): (i) modify, incorporate or use in any other works, translate, reverse engineer (except to the limited extent applicable statutory law expressly prohibits reverse engineering restrictions), decompile, disassemble, otherwise attempt to derive source code from or create derivative works based on the Products; (iii) make unauthorized copies of the Products; (iv) disclose, distribute, transfer or market the Products to third parties; (v) remove any proprietary notices, labels or marks on or in any copy of the Products; or (vi) use the Products other than as permitted herein.

3. Support and Maintenance. Provided End User has an active and fully paid contract for Support and Maintenance, Imperva will provide Support and Maintenance in accordance with its standard Support and Maintenance terms then in effect.

4. Additional Terms for Services.

a. Accessing Services. Except as explicitly set forth herein, End User is solely responsible for acquiring and maintaining all of the equipment, software, services and items necessary to access and make use of the Services, including without limitation paying all charges, taxes, and other costs and fees related to the Internet access. End User may access the Services only through the interfaces and protocols provided or authorized by Imperva and its partners and agrees to set-up, maintain and use the Services in strict compliance with Imperva's and its partners' instructions. End User is solely responsible for maintaining the confidentiality of any passwords and account information required to access Services, for all acts that occur in connection with End User's account and to immediately notify Imperva of any unauthorized use of End User's account. In the event of expiration or termination of any Services that require DNS routing, End User will be solely responsible for rerouting its DNS traffic and Imperva, its partners and suppliers shall have no liability for End User's failure to do so.

b. Authorization. Certain Services are offered to cache, serve, monitor and optimize web pages and web sites. As such, End User hereby grants Imperva and its partners a nonexclusive, worldwide, fully paid-up, royalty-free license to use, host, transfer, display, make available to the public, modify and otherwise exploit the content and material on End User websites ("End User Content"), in any media formats, solely for the purpose of providing of the Services. Imperva and its partners do not provide backup services for End User Content and if End User's use of the Services terminates for any reason, Imperva and its partners may, without notice, delete or deny End User access to any of content or meta data that may remain in its/their possession or control. In addition, End User agrees that if, at Imperva's and its partners' sole discretion, End User is using the Services in a manner that violates laws, rules or regulations or creates an excessive burden or potential adverse impact on Imperva's, its partners' or its suppliers' systems, business or customers, Imperva, its partners or its suppliers may suspend or terminate End User's access to the Services without notice to or liability to End User.

5. Professional Services. Professional Services, if any, to be provided by Imperva to an End User will be subject to a separate a statement of work ("SOW") agreed to by Imperva and Imperva's standard Professional Services terms then in effect.

6. Fees, Payment Terms. End User shall pay Imperva (or its authorized reseller) the applicable fees designated by Imperva (or its authorized reseller). Overage fees may apply if End User exceeds its allowance for any Product. Any fees payable to Imperva are non-refundable and payable in US Dollars. End User shall also pay all sales, use, value-added and other taxes, tariffs and duties of any type assessed against End User, except for taxes on Imperva's income. Fees shall be invoiced as follows: (a) fees for all Services and Support and Maintenance shall be invoiced in advance of the applicable Service or Support and Maintenance period, (b) fees for Software licenses and Appliance purchases will be invoiced upon Delivery. Title to Appliances and risk of loss shall pass to End User upon Delivery and Products shall be deemed accepted by End User upon Delivery. All payments from End User to Imperva are due net thirty (30) days of date of receipt of invoice. If End User's account for Services and Maintenance and Support Services is thirty (30) days or more overdue, in addition to any of its other rights or remedies, Imperva reserves the right to suspend the Services provided to End User, without liability to End User, until such amounts are paid in full. Imperva shall have the right to conduct and/or direct an independent accounting firm to conduct, during normal business hours, an audit of End User's facilities, computers and records to confirm End User's use of Products is in compliance with this Agreement. End User shall provide reasonable cooperation with any such audit.

7. Confidentiality; Privacy. End User agrees to hold confidence, during the term of this Agreement and for three (3) years after the termination hereof, any and all confidential and proprietary information of Imperva and its partners (the "Confidential Information"). Confidential Information includes, without limitation, the Products, their performance (including any benchmarking information) and Imperva's pricing of the Products. End User agrees not to use the Confidential Information except as necessary to fulfill its obligations or exercise its express rights hereunder, and not to disclose the Confidential Information to any person (other than End User's personnel having a need to know) without the prior written consent of Imperva. Without granting any right or license, Imperva agrees that the foregoing shall not apply with respect to any information that End User can document (i) is or becomes (through no improper action or inaction by End User or any affiliate, agent, consultant or employee of End User) generally available to the public, or (ii) was in its possession or known by it without restriction prior to receipt from Imperva. End User may make disclosures required by law or court order provided End User uses diligent reasonable efforts to limit disclosure and to obtain confidential treatment or a protective order and allows Imperva to participate in the proceeding.

Imperva may collect, store and use information obtained from End Users to provide and improve the Products. Please read our Privacy Policy available at www.imperva.com/other/legal.

8. Proprietary Rights. All title and intellectual property rights in and to the Products and Confidential Information is owned exclusively by Imperva and its partners and suppliers. Other than as expressly set forth in this Agreement, no license or other rights in or to the Products and intellectual property rights thereto are granted to End User, and all such licenses and rights are hereby expressly reserved.

9. Warranty and Disclaimer.

a. Imperva warrants that during the sixty (60) day period commencing on the date of first Delivery, the Software and the Appliances will perform materially in accordance with their Documentation. In the event of a breach of the foregoing warranty with respect to the Software, as End User's sole and exclusive remedy, Imperva shall, at its sole expense, use reasonable efforts to modify the Software, so that it performs materially in accordance with its Documentation. In the event of a breach of the foregoing warranty with respect to an Appliance, as End User's sole and exclusive remedy, Imperva shall, at its sole expense and at its option, repair the Appliance or replace the Appliance with a new or reconditioned Appliance that performs materially in accordance with its Documentation. The foregoing warranty extends only to the original purchaser and will not apply to the misuse of or damage to the Products. The rights and remedies granted End User under this Section state Imperva's entire liability, and End User's exclusive remedy, with respect to any breach of the warranty set forth in Section 9(a).

b. EXCEPT AS EXPRESSLY SET FORTH IN SECTION 9(a), THE PRODUCTS, THE SUPPORT AND MAINTENANCE SERVICES OR THE PROFESSIONAL SERVICES ARE PROVIDED "AS IS' AND IMPERVA MAKES NO WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE. IMPERVA, ITS PARTNERS AND SUPPLIERS MAKE NO WARRANTY THAT USE OF THE PRODUCTS, THE SUPPORT AND MAINTENANCE SERVICES OR PROFESSIONAL SERVICES WILL BE UNINTERRUPTED, ERROR-FREE OR DEFECT-FREE, OR AVAILABLE AT ALL TIMES. IMPERVA HEREBY SPECIFICALLY DISCLAIMS, ON BEHALF OF ITSELF AND ITS PARTNERS AND SUPPLIERS, ALL IMPLIED WARRANTIES, INCLUDING ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW.

10. Limitations of Liability. IN NO EVENT WILL IMPERVA'S (AND ITS PARTNERS OR SUPPLIERS') LIABILITY FOR DIRECT DAMAGES HEREUNDER EXCEED THE TOTAL VALUE OF AMOUNTS TO BE PAID BY END USER FOR THE PRODUCT OR SERVICE AT ISSUE. IN NO EVENT SHALL IMPERVA HAVE ANY LIABILITY TO END USER FOR ANY LOST PROFITS, LOSS OF USE, INTERRUPTION OF THE SERVICES, COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES HOWEVER CAUSED AND, WHETHER IN CONTRACT, TORT OR UNDER ANY OTHER THEORY OF LIABILITY, WHETHER OR NOT THE PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

11. Term and Termination.

a. The term of this Agreement will commence upon Imperva making the Products available to End User and will continue in effect for such time as End User continues to have the right to access the Products. Support and Maintenance for Software and/or Appliances will automatically renew at the end of the applicable Support and Maintenance term unless either party gives the other at least thirty (30) days notice of non-renewal prior to the end of the then current term.

b. Either party may terminate this Agreement due to a material breach of this Agreement by the other party if such material breach remains uncured for a period of thirty (30) days following receipt of written notice by the breaching party; provided that Imperva may terminate this Agreement and/or all licenses granted to End User hereunder immediately upon written notice to End User if End User breaches any provision of Section 2 (License & Restrictions), Section 4 (Additional Terms for Services) or Section 7 (Confidentiality). In addition, Imperva may terminate any trial, evaluation or demonstration rights granted to End User at any time, with or without notice.

c. Upon the earlier of expiration of End User's rights or termination of the Agreement, Imperva will cease providing all Services, Support and Maintenance and any Professional Services, and each party shall promptly return or destroy the other party's Confidential Information. Termination shall not relieve End User of the obligation to pay any fees accrued or payable to Imperva prior to the effective date of expiration or termination. The following sections shall survive termination of this Agreement: Sections 2(c), 4, 6 -13, and 15.

12. Government End User. If End User is part of an agency, department, or other entity of the United States Government ("Government"), the use, duplication, reproduction, release, modification, disclosure or transfer of the Software and Product is restricted in accordance with the Federal Acquisition Regulations as applied to civilian agencies and the Defense Federal Acquisition Regulation Supplement as applied to military agencies. The Product and Software are each a "commercial item," "commercial computer software" and "commercial computer software documentation." In accordance with such provisions, any use of the Product or Software by the Government shall be governed solely by the terms of this Agreement. All other use is prohibited.

13. Compliance With Laws; Export. End User agrees to abide by all applicable local, state, national and international law and regulations, and not to use the Services for any purpose that is unlawful, not contemplated or prohibited under this Agreement. End User shall comply with all export laws and restrictions and regulations of the Department of Commerce, the United States Department of Treasury Office of Foreign Assets Control ("OFAC"), or other United States or foreign agency or authority, and End User shall not export, or allow the export or re-export of the Software, Appliance Product or Services in violation of any such restrictions, laws or regulations. End User agrees to the foregoing and

represents and warrants that End User is not located in, under the control of, or a national or resident of any restricted country. End User agrees to indemnify and hold Imperva, its partners and suppliers harmless against any claims, losses or expenses arising out of End User's breach of this Agreement or use of the Products.

14. End User Mention. End User consents to Imperva using its name and logo to identify End User as a customer of Imperva, such as use on Imperva's website. Any use shall be subject to Imperva complying with any guidelines that End User may deliver to Imperva from time-to-time regarding the use of its name and logo. This consent terminates upon termination of the Agreement.

15. Miscellaneous Provisions. The parties are independent contractors under this Agreement and nothing in this Agreement authorizes a party to act as an agent of the other or bind the other to any transaction or agreement. This Agreement may not be assigned in whole or in part, by operation of law or otherwise, without the prior written consent of the other party, provided that a party may freely assign this Agreement in connection with a merger, acquisition, reorganization or reincorporation of such party with notice to the non-assigning party. In the event any provision of this Agreement shall be determined to be invalid or unenforceable under law, all other provisions of this Agreement shall continue in full force and effect. This Agreement contains the entire agreement of the parties with respect to the subject matter of this Agreement and supersedes all previous communications, representations, understandings and agreements, either oral or written between the parties with respect to said subject matter. This Agreement may only be modified or waived in a written instrument signed by both parties. A waiver of any breach under this Agreement shall not constitute a waiver or any other breach or future breaches. Notwithstanding the foregoing, if a separate, written and signed agreement for the license of the Products exists between End User and Imperva, the terms of that written agreement (excluding any pre-printed terms of any Purchase Order, confirmation or similar document, all of which will have no effect and will not be considered agreed to by Imperva) shall take precedence over this Agreement. All notices, requests, demands and other communications hereunder shall be in writing and shall be deemed to have been duly given if delivered or mailed by certified mail, return receipt requested or by any other means of delivery which generates a written receipt at the addresses set forth on the cover sheet. This Agreement will be interpreted and construed in accordance with the laws of the State of California and the United States of America, without regard to conflict of law principles. The parties hereby consent to the exclusive jurisdiction and venue of the state and federal courts located in San Francisco County, California for resolution of any disputes arising out or relating to this Agreement.

16. Open Source Software. Open Source Software is copyrighted and licensed under the GPL/LGPL and other licenses. Copies of or references to those licenses are included with Software in the "Help" section. You may obtain the complete corresponding Open Source Software source code from us for a period of three years after our last shipment of the Software, by sending a money order or check for $10 to: Legal Department - Open Source Software Request, Imperva, Inc., Redwood Shores, CA 94065, United States.

Last updated: May 10, 2011

Table of Contents

Chapter 1 - Introduction **20**
- **Using this Guide** **21**
  - Intended Audience 21
  - What This Publication is About 21
- **The Admin Workspace** **23**
- **Document Conventions** **24**

Chapter 2 - Topologies and Deployment **25**
- **Choosing a Deployment** **26**
  - CPU Affinity 26
- **Sniffing Mode** **28**
  - Topologies 28
- **Inline Gateways** **29**
  - Bridge Deployments 29
    - Topologies 29
  - Fail Safe and Fail Open Modes 29
- **Reverse Proxy Deployments** **30**
  - Reverse Proxy Overview 30
    - Reverse Proxy Mode Advantages 30
  - Transparent Reverse Proxy Overview 30
    - Transparent Reverse Proxy 30
    - Transparent Reverse Proxy - Selected Web Servers 31
  - Non-Transparent Reverse Proxy Overview 32
    - Kernel Reverse Proxy (KRP) 32
    - Kernel Reverse Proxy (“One Arm”) 33
    - Apache Reverse Proxy (ARP) 33
    - Apache and Kernel Reverse Proxy on the Same Gateway 33
  - Reverse Proxy with Load Balancer 34
- **Features Available in the Each Deployment Mode** **36**
- **Guidelines** **38**
  - Gateways 38
  - Management Servers 38
  - Remote Agents 38

Chapter 3 - Platforms and Installation **39**
- **Forward Compatibility** **40**
- **Preparing the Appliance** **41**
- **Installing the SecureSphere Software** **42**
  - G Series Appliances (Except G2 and G2-2) 42
    - Installation Monitoring 42
    - Installing From The Network 42
    - Installing From USB 42
    - Connecting to the G Series Appliance Using a Serial Console 43
  - G2 and G2-2 Appliances 44
    - Installation Monitoring 44
    - Installing From The Network 44
    - Installing From USB 44
    - Installing Using an External CD Drive 45
    - Connecting to the G2 or G2-2 Appliance Using a Serial Console 45
  - X and M Series Appliances 46
    - Connecting to a X or M Series Appliance Using a Serial Console 46
    - Installing From USB 46
    - Installing From The Network 47
  - Creating a Bootable USB Device Containing the Installation Image 47
- **After Installing the SecureSphere Software** **49**
  - Management Servers 49
    - Connecting to the Management Server 49
    - MySQL Users 49

Chapter 4 - Configuring SecureSphere 50
Initial Configuration 51
IPv6 52
SecureSphere Features Which Support IPv6 52
Overview 52
IPV6 Address Formats 52
CIDR Notation 53
IPv4 / IPv6 Dual Stack 53
SecureSphere MX and Gateway 53
Hostnames 53
IPv6 in impcfg and impctl 53
Exceptions 54
External Systems 55
SecureSphere Users 56
The Different SecureSphere Users 56
Appliance OS 57
CLI Users 57
Authentication Failure 57
Passwords 57
Timeout 58
Date Changes 58
Gateway/Management Server Appliance Initial Configuration 59
First-Time Login (Configuration) 59
Registering a Gateway 59
Configuring SecureSphere Using the Command Line Tools 60
Command Line Tools and MX-HA 60
Changing MX Properties in an MX-HA Environment 60
Stopping and Starting the MX in an MX-HA Environment 60
impcfg 61
Top Screen 61
impcfg Functionality Map 63
Configuring a Management Server 69
Configuring a Gateway 71
Gateway Actions 72
Configuring a Gateway as a Bridge 73
Configuring a Gateway as a Sniffing Gateway 75
Managing Remote Agents 76
Adding a Legacy (pre-version 7.0) Remote Agent 77
Modifying a Legacy (pre-version 7.0) Remote Agent 78
Deleting a Legacy (pre-version 7.0) Remote Agent 78
Adding a Remote Agent Listener 78
Deleting a Remote Agent Listener 79
Adding a SecureSphere Agent for DB2 z/OS Listener 79
Deleting a SecureSphere Agent for DB2 z/OS Listener 79
Managing Remote Agent Related Routes 80
Configuring a Data Assessment Server (DAS) 81
Reconfiguring the DAS as a Onebox 83
Configuring the Platform 84
Network Management 85
Management Interface 86
LAN Interface 88
Default Gateway 89
Static Routes 89
Name Resolution (DNS client) 90
Locate Network Devices 91
Time Management 91
Time Servers 92
Users Management 92
Change Root User Password 93

Create New User 94
Manage User 95
Configure RADIUS Authentication 96
Enable / Disable RADIUS 96
Edit External Authentication Configuration 97
Hostname Management 97
Bootloader Password Management 98
Configuring SecureSphere Routes 99
Configuring Remote Agent Routes 99
Configuring VRRP Routes 100
Configuring Transparent Reverse Proxy 102
Configuring Kernel Reverse Proxy 103
Before Configuring the Kernel Reverse Proxy 103
Configuring the Kernel Reverse Proxy 103
Changing the Gateway's Mode to KRP 103
Configuring Aliases 105
Configuring Routing 107
Configuring a Server Group and Service 108
Configuring KRP and Decision Rules 108
Configuring High Availability for KRP 108
Configuring the Gateway for High Availability 108
Configuring the Management Server for High Availability 109
Configuring Apache Reverse Proxy 110
Changing the Gateway's Mode to ARP 110
Configuring ARP 110
RSA Clear Trust Single Sign On (SSO) 112
RSA Clear Trust Overview 112
Installing the RSA Access Manager Agent on the SecureSphere Gateway 113
Configuring Kernel Reverse Proxy and Apache Reverse Proxy on the Same Gateway ... 117
Switching Deployments 118
Overview 118
From a Onebox to a Gateway 118
From a Gateway to a Onebox 118
Changing the MX of a Gateway 118

Chapter 5 - Installing Remote Agents 120
Remote Agent Configuration Tasks 121
Installing the Remote Agent 122
Preparing for Installation 122
Obtaining the Latest Version of the Remote Agent 122
Verifying Prerequisites 123
Preparing the Database 124
Configuring the SecureSphere Gateway Before Installation 125
Configuring Listeners 125
Manage Remote Agent Related Routes 126
Installing the Remote Agent 127
Installing the Remote Agent on a non-Windows System 128
Special Considerations for SUSE and OEL UEK Platforms 130
Installing the Remote Agent on a Windows System 131
Silent Installation Parameters 133
After Installing the Remote Agent 135
Data Interface Discovery and Configuration 136
MSSQL Post Installation Information 137
Oracle - Windows Post Installation Information 137
DB2 - AIX Post Installation Information 137
AIX Post Installation Information 137
First-Time Configuration Wizard 137
Registering the Remote Agent to a SecureSphere Gateway 138

Uninstalling the Remote Agent 141
Uninstalling the Remote Agent on a non-Windows System 141
After Uninstalling the Remote Agent on a non-Windows System 141
AIX 141
Linux, Solaris and HP-UX 142
Uninstalling the Remote Agent on a Windows System 142
Upgrading the Remote Agent 143
Upgrading the Remote Agent on a non-Windows System 143
Upgrading the Remote Agent on a Windows System 143
Starting and Stopping the Remote Agent 144
Starting and Stopping the Remote Agent from the Management Console 144
Starting the non-Windows Remote Agent from the Command Line 144
Stopping the non-Windows Remote Agent from the Command Line 145
Starting the Windows Remote Agent from the Command Line 145
Stopping the Windows Remote Agent from the Command Line 145
Remote Agent Management Console 146
Remote Agent Management Console Conventions 146
Starting the Remote Agent Management Console 147
Registering the Remote Agent to the Gateway 147
Activating Settings Manually 148
Agent Information Displayed in the Console 149
Agent Troubleshooting Using the Management Console 149
Show Counters 149
Working with High Availability 150
Configuring the Gateways to Operate in the HA Mode with Agents 150
Configuring the Remote Agent to Operate in the HA Mode 152
Diagnostic Tools 153
Remote Agent Logs 153
Remote Agent Error Messages 153
Maintenance Tasks 154
Remote Agents in a Hypervisor (Virtualized) Environment 154
If the MAC Address Changes 154
Prerequisite Tests for non-Windows Agents 155
Supported Interfaces for the Gateway Listener 160
Advanced Agent Configuration 161
UDP Tunnel Mode 161
High Availability in UDP Mode 162
UDP Listener Configuration 162
Working with a NATed Listener 163
Working with a NATed Listener in Non-Windows Environments 163
Working with a NATed Listener in Windows Environments 164
Working with Multiple Oracle Instances 165
Monitoring Solaris Zones Using Remote Agents 166
Monitoring MySQL Traffic 167
RWorking with DAC (Dedicated Administrator Connection) 167
Command Line Scripting Language 168
Conventions for Command Line Scripting 168
Syntax for Command Line Scripting 169

Chapter 6 - Installing SecureSphere Agent for DB2 z/OS 172
Installing SecureSphere Agent for DB2 z/OS - Version 2.1 173
Upgrading from Version 1.3 to Version 2.1 173
Configuring SecureSphere Agent for DB2 z/OS Tasks 173
Before Installing and Configuring SecureSphere Agent for DB2 z/OS 174
Information You Must Have Before You Begin 174
Terminology Used In This Guide 174
Roles and Assignments for the Installation and Configuration 175
Mainframe Software Requirements 176
Security Requirements 176

TCP/IP Requirements 177
Optimizing Performance 177
Supported Facilities 177
Downloading and Installing SecureSphere Agent for DB2 z/OS 177
Downloading and Installing the Product 178
APF Authorizing the LOAD Library 179
Creating the ADMIN Library 179
Configuring SecureSphere Agent for DB2 z/OS (on z/OS) 180
Accessing the Product Customization Facility 180
Specifying the License Key 181
Specifying the Product Libraries 182
Specifying the Customizable Parameters 182
Detailed Information About the Customization Parameters 184
Completing the Configuration 187
Starting, Managing, and Stopping SecureSphere Agent for DB2 z/OS 189
Requirements and Restrictions for Starting SecureSphere Agent for DB2 z/OS 189
Modifying the Started Task Procedure and Starting the Started Task 189
Using Operator Commands to Stop and Manage the Product 189

Installing SecureSphere Agent for DB2 z/OS - Version 1.3 191

Configuring SecureSphere for z/OS Tasks 191
Before Installing and Configuring SecureSphere Agent for DB2 z/OS 191
Information You Must Have Before You Begin 192
Terminology Used In This Guide 192
Roles and Assignments for the Installation and Configuration 192
Mainframe Software Requirements 194
Security Requirements 194
TCP/IP Requirements 194
Optimizing Performance 194
Supported Facilities 194
Downloading and Installing SecureSphere Agent for DB2 z/OS 195
Downloading and Installing the Product 195
APF Authorizing the LOAD Library 198
Creating the ADMIN Library 198
Including the Product Libraries in Your Disaster Recovery Plan 198
Configuring SecureSphere Agent for DB2 z/OS (on z/OS) 199
Accessing the Product Customization Facility 199
Specifying the License Key 200
Specifying the Product Libraries 201
Specifying the Customizable Parameters 201
Detailed Information About the Customization Parameters 203
Completing the Configuration 205
Authorizing the Started Task for the Product 206
Binding Packages for the Product 206
Initializing and Securing the Rules Data Set 207
Specifying the Priority Using WLM 207
Starting, Managing, and Stopping SecureSphere Agent for DB2 z/OS 207
Requirements and Restrictions for Starting SecureSphere Agent for DB2 z/OS 208
Modifying the Started Task Procedure and Starting the Started Task 208
Using Operator Commands to Stop and Manage the Product 208

Chapter 7 - Gateways 210

Configuring Gateways and Gateway Groups 211

Gateways 211
Gateway Details 211
Remote Agent Details in the Gateways Window 213
Log Collectors Details in the Gateways Window 213
Configuring Archiving per Gateway 214
Gateway Groups 215
Exporting Technical Information from Gateway and Onebox 219

Chapter 8 - Licenses **220**
License Overview **221**
Uploading Licenses **222**
Viewing Licenses **223**
Managing Database Scanning and Assessment Licenses **225**

Chapter 9 - Users and Permissions **227**
Understanding Permissions **228**
Permission Models in SecureSphere 228
Roles and Users 228
Permission Types 229
Understanding the Permissions Window 231
Adding and Removing Permissions 232
Notes on Permission Behavior 232
Permissions Workflow **233**
Working with Roles **234**
PreDefined Roles 234
Custom Role Examples 234
Creating a Role 235
Working with Users **237**
Creating a SecureSphere User 237
Assigning Roles to Users 238
Configuring Object or Category Level Permissions 238
Understanding How Permissions are Displayed 239
Configuring Permissions Navigation and Activate Settings 241
Configuring User Information 242

Chapter 10 - Sessions **244**
Connected Users **245**
Sessions 245

Chapter 11 - ADC **246**
Viewing ADC Content and Status **247**
Updating ADC Content **249**
ADC History **250**

Chapter 12 - Job Status **252**
Jobs Status **253**
Displaying the Jobs Status Window 253
Editing a Job 254
Aborting a Job 254

Chapter 13 - Maintenance **255**
Audit Fast Viewing **256**
Audit Purge **257**
Assessment Results Archive **258**
Discovery Results Archive **260**
Exporting and Importing the Management Server **262**
Export Using the SecureSphere GUI 262
Export / Import Manually Using the Interactive CLI 264
Listing the Contents of an Exported File 265
Export / Import Manually Using the Non-Interactive CLI 265
Miscellaneous Maintenance Tasks 267

Reports Archive **269**
Risk Score Update **270**
Kerberos Key Update **271**
System Events Archive **272**
Vulnerabilities Purge **274**
Extracting Archives for Viewing **275**
Audit Archive Conversion **276**
Exporting an Archive to TAR Format with CSV Values 276
Converting an MPRV file to TAR Format with CSV Values 277
Analyzing Converted Files 277
Data Format 278
Relationship between Tables 280
Sample Queries 280

Chapter 14 - System Definitions **285**
Dynamic Profiling **287**
Learning Exceptions 287
Profile Optimization 287
Profile Size Limits 288
Switching to Protect Mode Thresholds (SQL) 291
Switching to Protect Mode Thresholds (Web) 294
Gateway Settings 295
Audit Settings 296
Response Page Display in Alerts Settings 296
Web to Database User Tracking Settings 296
Security and Authentication **298**
Authentication and Authorization Configuration 298
FIPS Settings 298
Password Settings 299
SSL Certificate Expiration Monitoring 300
Management Server Settings **301**
Action Interfaces 301
Creating and Configuring Action Interfaces 302
Agents 303
Alert Aggregation Configuration 304
Application Groups Settings 305
Assessments 305
CSV Upload Default Settings 305
Data Owner Settings 306
External HTTP Settings 306
External Systems 307
Defining External Systems 307
External Systems - Active Directory Collection (Forest) 309
External Systems - Kerberos Authentication 310
External Systems - LDAP 313
External System - LDAP Authentication and Authorization 313
External System - RADIUS Authentication 315
External System - SQL 316
External System - SSH Proxy 316
File URM 317
Keywords Settings 317
Log Collectors 319
Defining Log Collectors 319
Log Collector Parameters 320
Lookup Data 320
Policy Settings 321
Report Settings 321
Server Definitions 322
Stored Procedures Settings 322

System Events Notifications 323
User Interface Settings 325
Display Limits 325
Language Settings 325
ThreatRadar Settings 326
General Settings 326
Miscellaneous Audit Data Operations 327
Changing the Audit Directory Path 327
Configuring Encryption 328

Chapter 15 - System Performance 329
Management Server 330
Exporting Technical Information from Management Servers 332
Gateways and Agents 333
Troubleshooting Performance 335
Management Server 335
Gateways and Agents 335
System Performance - CPU Load 336
System Performance - Policies 336
System Performance - Signature and Dictionaries 336
System Performance - SSL 336
System Performance - Agents 336

Chapter 16 - Gateway High Availability 339
Layer 2 High Availability Deployments 340
At the Network Level 340
Link Aggregation (Etherchannel) 340
At the SecureSphere Level 340
IMPVHA Protocol — Active-Passive and Active-Active Failover 341
Bridge STP 341
Bridge STP — Active-Passive Failover 342
Bridge STP — Active-Active Failover 342
Redundant Architecture (STP) — Configuration 343
Layer 3 (Proxy) High Availability Deployments 344
At the Network Level 344
Load Balancer Integration 344
At the SecureSphere Level 345
Redundant Architecture (VRRP) — Configuration 345
Other High Availability Deployments 346
Fail-Open Bridge 346
Fail Open — Configuration 346
Sniffing Gateway High Availability 346

Chapter 17 - Management Server High Availability (MX-HA) 349
Management Service-High Availability (MX-HA) Overview 350
Management Server-High Availability (MX-HA) Implementation 351
Management Server High Availability (MX-HA) Components 352
Linux Heartbeat 352
Oracle Standby Database (Data Guard) 352
SecureSphere Server 352
HA Health Check 352
Imperva Watchdog 352
Before Installing Management Server High Availability (MX-HA) 353
Hardware and Software Requirements 353
Pre-Installation Tasks 353
Install the Latest Patch 353

Configure the Interconnected Interfaces 353
Test the Interconnected Interfaces 354
Download the RPMs and Prepare the Servers 354
Set Up Hostnames 355
Configure SSH Trust for User Root 356
Configure SSH Trust for User Oracle 357
Installing Management Server High Availability (MX-HA) 359
After Installing Management Server High Availability (MX-HA) 362
Verify the Primary Server is Active 362
Register the Gateway 362
admin-ips 362
Re-registration 363
Uninstalling MX-HA 363
Changing Database and/or System Passwords 364
Monitoring Management Server High Availability (MX-HA) 365
MX-HA Status 365
Confirming that MX-HA is Correctly Configured 365
Initiating a Failover in an MX-HA Environment 365
Confirming That the MX-HA Servers are Synchronized 366
MX-HA Logs 367
healthCheck.log 367
/var/log/ha-log 367
alert_secsph.log 367
Heartbeat Statuses 367
Resource Status 367
Server Status 368
impctl watchdog 368
Heartbeat Behavior 368
Failover Sequence 368
Standby Recreation 369
Known Issues 369
MX-HA Installation Failure 369
Failure While Building the Standby Database 369
Management Server Replacement 369
File List 370

Chapter 18 - Network High Availability 372
Network High Availability Support 373
Configuring Network High Availability 373

Appendix A - Installing SecureSphere From the Network 374
Installing from the Network 375
Introduction 375
Preparing the Deployment Server 376
Obtaining the Network Deployment Package 376
Installing the Package on the Deployment Server 376
Configuring the Deployment Server IP Address 376
Running a Network Deployment 378
Connecting the Target Appliance and Deployment Server 378
Running the Deployment Program on the Deployment Server 379
Booting the Target Appliance 380
Monitoring Installation Progress 382
Finalizing Installation 382
Reconfiguring the G2 and G2-2 Appliance Not to Boot from the Network 383
Frequently Asked Questions 383
Serial Console Installation 384

Appendix B - Network Services 385

SecureSphere Component Communication **386**
Configuring Firewall Ports **387**
Serial Console Access to SecureSphere **388**
Supported Versions and Upgrades 388
Hardware 388
Software 388
Upgrades 388
Supported Serial Console Settings 388
Before You Begin: Checking OS Layer Serial Console Access 389
Configuring BIOS Settings for Serial Console 389
Editing the GRUB Configuration File 390
SecureSphere Network Installation with Serial Console 391

Appendix C - SAP Configuration **392**
Configuring the SecureSphere Gateway **393**
Universal User Tracking **394**
Monitoring SAP Transactions **395**
Defining SAP Transactions 396
Configuring SAP Transactions for use in SecureSphere 396
Other Audit Policies 397
Database Table Groups **398**

Appendix D - Add-Ons **399**
Hardware Security Modules (HSM) **400**
nCipher Card 400
Installing the nCipher Card 400
Installing the nCipher Card Driver 400
Verifying the Installation 400
Security World Initialization 402
Importing Keys 403
Update the Gateway HSM 405
Update the Server with the Certificate Key 405
nCipher netHSM 406
High Level Functional Description 406
Components Taking Part in the Integration 406
High Level Installation Process 407
nCipher HSM Installation 407
Setting Up the Integration 408
Basic netHSM Configuration 409
SafeNet LunaSA 411
High Level Functional Description 411
LunaSA High Level Installation Process 411
LunaSA Software Installation 412
Storage Area Networks (SAN) **422**
SAN Overview 422
Supported SAN Hardware 422
Host Bus Adapters 422
Cabling 422
Configuring SecureSphere for SAN 423
SAN Configuration Task Overview 423
Determine Storage Requirements 424
Make a Note of the Original SCSI Configuration 424
Add the HBA to the SecureSphere Appliance 425
Check the HBA Card 425
Request that the Storage Manager Add a Logical Volume 426
Physically Connect to the SAN 427
Scan the Fibre Channel 427
Update /etc/modprobe.conf 428
Create a File System on the SCSI Target 429
Mount the New File System 429

Test the New File System 429
Create a Startup File 429
Reboot the Machine 431
Configure SecureSphere to Use the SAN 431
Disabling the SAN 431
On the Management Server 431
On the Gateway 431
SSL Accelerator 433
LOM (Lights Out Management) 434
Overview 434
Connecting to the LOM 434
Managing the LOM 434
General 435
Network 436
Security 437
ANMS (RADIUS Settings) 438
User Management 439
Customization 440
Firmware 441
Power Management 442
Log 443
Logout 444

Appendix E - Command Line Interface 445
impcfg 446
impcfg Functionality Map 446
impctl 452
"Safe" impctl Commands 452
Stopping and Starting the MX in an MX-HA Environment 453
Miscellaneous impctl Commands 453
Miscellaneous Commands 455
Powering Down the Appliance 455
Changing the Password for Management Server - Gateway Communication 455

Appendix F - FIPS 140 Compliance 457
Compliance 458
2.1 Encrypted Communications 458
2.2 MX Encrypted Communications 458
2.2.1 FIPS-Approved Algorithms 458
2.2.2 FIPS-Non-Approved Algorithms 458
2.3 SecureSphere Gateway and Platform Communications 459
2.3.1 FIPS-Approved Algorithms 459
2.3.2 FIPS-Non-Approved Algorithms 459
2.4 HSM solution 459
2.5 SecureSphere WAF in FIPS Mode 459
Limitations 460
Activating FIPS Mode 461

Appendix G - Disaster Recovery 462
Disaster Recovery 463
Preparing for Disaster Recovery 463
Recovery 463
Automatically Re-registering the Gateways 464

Appendix H - PCI Compliance 465
PCI Data Security Standard 466
SecureSphere and PCI DSS 466
PCI Compliance 467
Protecting the SecureSphere Appliance 467

Protecting Cardholder Data 467

CHAPTER 1

Introduction

This chapter includes the following information:

- Using this Guide on page 21
- The Admin Workspace on page 23
- Document Conventions on page 24

Using this Guide

Intended Audience

This publication is intended for system administrators who are tasked with the installation, configuration and ongoing maintenance of Imperva SecureSphere.

What This Publication is About

This publication describes the functionality of the Imperva SecureSphere and provides information on its installation, deployment, configuration and maintenance.

This Administration Guide comprises the following chapters:

Administration Guide Chapters and Appendices

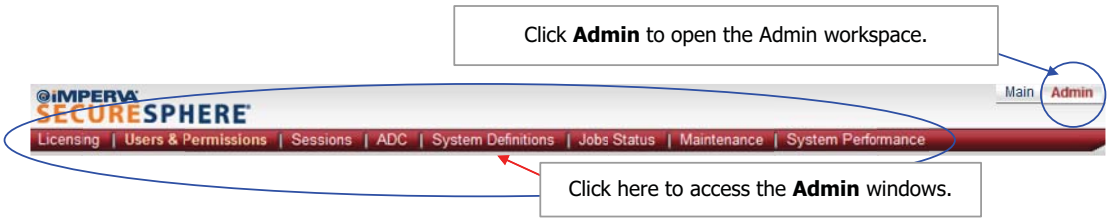
Chapter or Appendix Name	Description
Chapter 1, Introduction	This chapter describes the ***SecureSphere Administration Guide***.
Chapter 2, Topologies and Deployment	This chapter describes the different ways that SecureSphere can be deployed to protect Web and database applications.
Chapter 3, Platforms and Installation	This chapter describes how to install SecureSphere.
Chapter 4, Configuring SecureSphere	This chapter describes how to configure SecureSphere appliances.
Chapter 5, Installing Remote Agents	This chapter describes how to install SecureSphere Remote Agents.
Chapter 7, Gateways	This chapter describes how to configure SecureSphere gateways.
Chapter 8, Licenses	This chapter describes the SecureSphere licensing process.
Chapter 9, Users and Permissions	This chapter describes how to define SecureSphere administrators, users and their privileges.
Chapter 10, Sessions	This chapter describes how to track SecureSphere sessions.
Chapter 11, ADC	This chapter describes how to configure SecureSphere to download content from Imperva's ADC (Application Defense Center).
Chapter 14, System Definitions	This chapter describes the SecureSphere system definitions.
Chapter 12, Job Status	This chapter describes how to track jobs initiated by SecureSphere.
Chapter 13, Maintenance	This chapter describes how to maintain, backup and restore SecureSphere.
Chapter 15, System Performance	This chapter describes the system performance data SecureSphere provides about management servers, gateways and database agents.
Chapter 16, Gateway High Availability	This chapter describes how to configure High Availability for SecureSphere gateways.
Chapter 17, Management Server High Availability (MX-HA)	This chapter describes how to configure High Availability for SecureSphere management servers.

Administration Guide Chapters and Appendices

Chapter or Appendix Name	Description
Appendix A, Installing SecureSphere From the Network	This appendix describes how to perform the initial installation of SecureSphere from the network or from a USB device.
Appendix B, Network Services	This appendix describes how to configure the network in which SecureSphere appliances are deployed.
Appendix C, SAP Configuration	This appendix describes issues related to SAP configuration.
Appendix D, Add-Ons	This appendix describes various SecureSphere add-ons, such as HSM, SAN *etc*.
Appendix E, Command Line Interface	This appendix describes the SecureSphere command line tools: **`impcfg`** and **`impctl`**.
Appendix F, FIPS 140 Compliance	This appendix describes SecureSphere's FIPS 140-x compliance.
Appendix G, Disaster Recovery	This appendix details disaster recovery procedures for the SecureSphere management server.
Appendix H, PCI Compliance	This appendix describes how SecureSphere can help administrators achieve PCI compliance for their sites.

The Admin Workspace

To perform administrative tasks in SecureSphere, open the **Admin** workspace, by clicking **Admin** in the upper right-hand corner.



The **Admin** workspace consists of the following windows:

Admin workspace

	Description	For more information, see
Licensing	Install SecureSphere licenses	Chapter 8, Licenses
User and Permissions	Define SecureSphere administrators, users and their privileges.	Chapter 9, Users and Permissions
Sessions	Track open SecureSphere sessions.	Chapter 10, Sessions
ADC	Configure SecureSphere to download content from Imperva's ADC (Application Defense Center).	Chapter 11, ADC
System Definitions	Define system-wide parameters.	Chapter 14, System Definitions
Jobs Status	Track jobs initiated by SecureSphere.	Chapter 12, Job Status
Maintenance	Export SecureSphere system data, maintain archives etc.	Chapter 13, Maintenance
System Performance	Monitor system performance.	Chapter 15, System Performance

To access one of these windows, click its name.



Note: The **Admin** tab is visible only to users with administrative permissions. For more information, see Chapter 9, Users and Permissions.

Document Conventions

In this document, the following typographical and formatting conventions are used:

Typographical and Formatting Conventions

Convention	Meaning	Example
`command`	The `monospaced font` is used for CLI commands or output, and for file names.	`cd /tmp`
|	separates optional values in lists	`oranges` | `apples`

CHAPTER 2

Topologies and Deployment

This chapter describes the different deployments of SecureSphere, and includes:

- Choosing a Deployment on page 26
- Sniffing Mode on page 28
- Inline Gateways on page 29
- Reverse Proxy Deployments on page 30
- Features Available in the Each Deployment Mode on page 36
- Guidelines on page 38

Choosing a Deployment

A SecureSphere gateway can be deployed either inline, where traffic passes through the SecureSphere gateway, or as a sniffing gateway, where traffic does not pass through the gateway but is copied to it for analysis. The most important differences between these deployments are:

- An inline gateway can block malicious traffic so that it never reaches the protected network, but on the other hand, it introduces some latency.
- A sniffing gateway introduces no latency, and it can prevent malicious traffic from reaching the protected network by issuing TCP resets to the server on its blocking interface.

Inline gateways can be deployed in a number of configurations:

- **transparent bridge**: The SecureSphere gateway acts as a transparent bridge, monitoring traffic entering and leaving the protected network and applying the various policies. In transparent bridge mode, the SecureSphere gateway can also act as a transparent reverse proxy for Web applications.
- **reverse proxy**: In addition to the bridge functionality, for Web applications the SecureSphere gateway can act as a reverse proxy, configured as:
  - Transparent Reverse Proxy – in bridge mode (see Reverse Proxy Deployments on page 30)

    Transparent Reverse Proxy is configured for specific Web services, so a SecureSphere gateway can act as a proxy for some services but not for others. For more information, see Transparent Reverse Proxy - Selected Web Servers on page 31.
  - Kernel Reverse Proxy – see Kernel Reverse Proxy (KRP) on page 32
  - Apache Reverse Proxy – see Apache Reverse Proxy (ARP) on page 33

    Additionally, Kernel Reverse Proxy and Apache Reverse Proxy can be deployed on the same SecureSphere gateway. For more information, see Apache and Kernel Reverse Proxy on the Same Gateway on page 33.



Note: Onebox mode (where both the SecureSphere management server and SecureSphere gateway are integrated in a single machine) is available for all deployments except High Availability.

Kernel Reverse Proxy and Apache Revere Proxy must be configured during installation, using **`impcfg`**. Additionally, configuring Apache Revere Proxy requires manually editing configuration files. For more information, see Chapter 4, Configuring SecureSphere.

SecureSphere gateways can also be deployed in High Availability mode. For more information, see Gateway High Availability on page 339.

SecureSphere gateways can also be deployed in conjunction with Load Balancers. For more information, see Reverse Proxy with Load Balancer on page 34.



Note: Database Agents, installed on the database server, enable SecureSphere to monitor local database traffic. DB Agents are compatible with both inline and sniffing gateways. For more information about DB Agents, see the ***SecureSphere User Guide***.

This chapter presents some typical examples of these deployments. Not all possible deployments are covered here.

CPU Affinity



Note: CPU affinity does not apply in sniffing mode.

For all SecureSphere gateways with more than one core, SecureSphere implements IRQ affinity (CPU affinity), meaning that each core handles interrupts from specific interfaces.

SecureSphere version 8.0 allocates cores to interfaces at boot time. Beginning with version 8.5, SecureSphere implements dynamic allocation of cores to 10G interfaces, depending on the load. For other interfaces, the boot time allocation remains unchanged.

Sniffing Mode

Topologies

In a sniffing mode deployment, traffic does not pass through the SecureSphere appliance but is only copied to it. A sniffing appliance can monitor both Web and database traffic, and blocks malicious Web traffic by issuing TCP resets to the server. A sniffing appliance's advantage is that it introduces no latency in either Web or database application traffic.

The disadvantages of sniffing mode are:

- Issuing TCP resets is not as dependable a method of blocking traffic as is dropping packets.
- Overloaded SPAN ports sometimes drop packets, so SecureSphere will not inspect them.

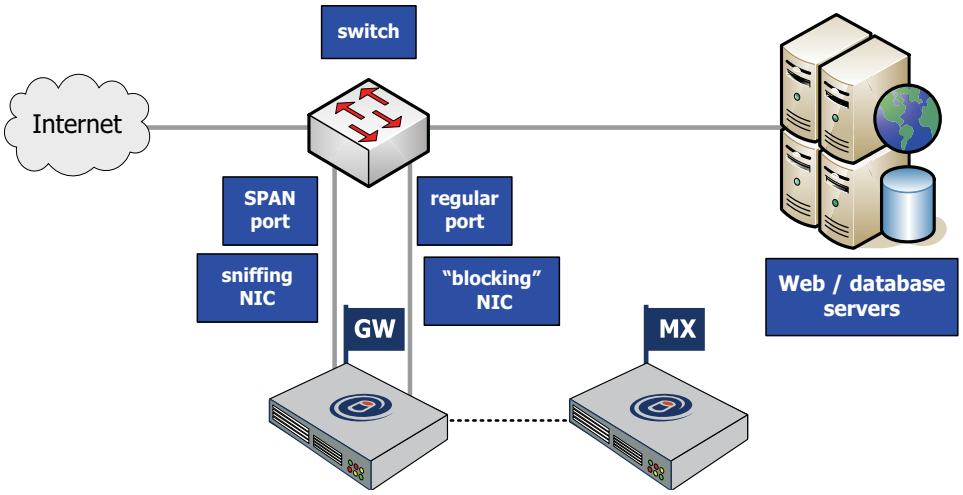


Figure 1 Sniffing Deployment

There are two methods to "sniff" the traffic:

- using a SPAN (mirror) port on the switch, or
- using a dedicated TAP

The SPAN port is less reliable since it depends on the switch resources and has lower priority than forwarding traffic, so it might miss packets. TAP does not have this disadvantage.

Aggregation taps can also be used.

Inline Gateways

Bridge Deployments

Topologies

In a bridge deployment, all traffic passes through the SecureSphere gateway, which monitors the traffic and blocks malicious connections by dropping packets.

SecureSphere supports two bridge topologies

- transparent bridge for DXG and WAF
- non-transparent bridge (for WAF only) using RP (transparent and non transparent RP)

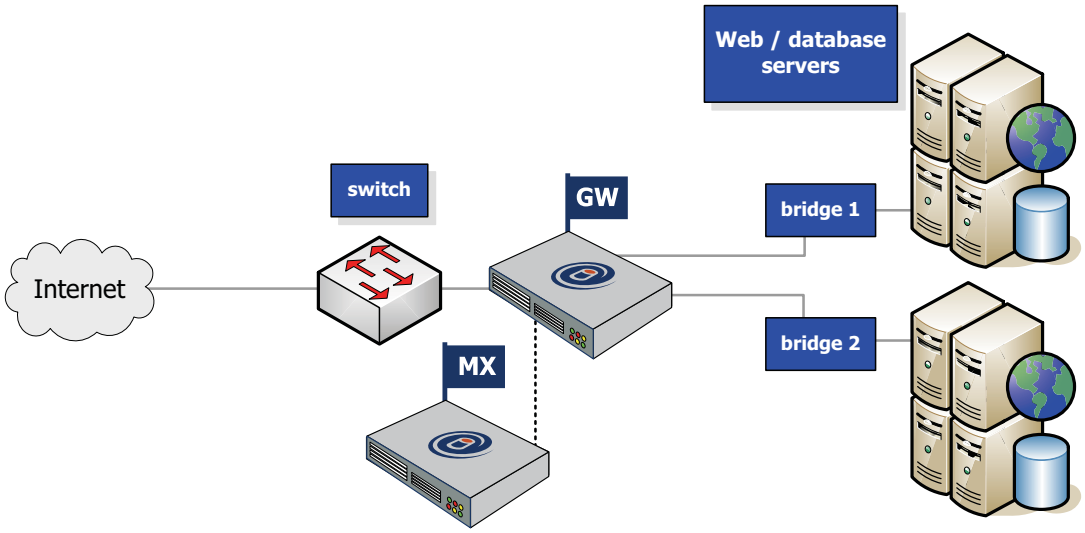


Figure 2 Inline Bridge Deployment

The bridge can be invisible (transparent) to both clients and servers, which would then see each others' real IP addresses.

Fail Safe and Fail Open Modes

A transparent bridge can be configured to maintain connectivity in the event of failure. In Fail Open mode, traffic will continue to pass through the bridge, but SecureSphere will not inspect it.

Reverse Proxy Deployments

For Web traffic only, an inline gateway can be configured as a Reverse Proxy. In a Reverse Proxy, traffic intended for a Web server first passes through the Reverse Proxy.

This section contains the following:

- Reverse Proxy Overview on page 30
- Reverse Proxy Mode Advantages on page 30
- Transparent Reverse Proxy Overview on page 30
- Transparent Reverse Proxy - Selected Web Servers on page 31
- Kernel Reverse Proxy (KRP) on page 32
- Kernel Reverse Proxy (“One Arm”) on page 33
- Apache and Kernel Reverse Proxy on the Same Gateway on page 33
- Reverse Proxy with Load Balancer on page 34

Reverse Proxy Overview

There are three kinds of Reverse Proxies:

- Transparent Reverse Proxy (TRP)
- two kinds of non-Transparent Reverse Proxies:
  - Kernel Reverse Proxy (KRP)
  - Apache Reverse Proxy (ARP)

Reverse Proxy Mode Advantages

Some of the advantages of Reverse Proxy mode are:

- A Reverse Proxy assembles packets into a complete message, inspects the message and confirms that it complies with the relevant policies, and only then transmits the packets to the server.
- Reverse Proxy mode supports features that require changing data, for example, cookie signing, SSL decryption, *etc*.
- Reverse Proxy mode supports features that require changing the destination IP address.
- Traffic is decrypted only once, by the SecureSphere. The server sees only unencrypted traffic, improving server performance.
- In the same way, SSL decryption is offloaded from the server to the SecureSphere gateway.
- Reverse Proxy mode enables SecureSphere to be implemented in legacy deployments without the need to reconfigure networks (drop-in replacement).

Transparent Reverse Proxy Overview

Transparent Reverse Proxy

In Transparent Reverse Proxy mode, the client is unaware of the Reverse Proxy, and connects directly to the server. The SecureSphere gateway is not visible to the client or to the server, which see each others’ real IP addresses.

The SecureSphere gateway is in bridge mode, but additionally functions as a Reverse Proxy for the servers specified in the SecureSphere GUI (in the **Transparent Reverse Proxy** section of the **Definitions** tab of the server group (**Main** > **Setup** > **Sites**). All other traffic, including non-Web traffic, is bridged through. In this way, the same SecureSphere gateway protecting many Web and database server groups can act as a

Reverse Proxy for some or all of the Web server groups it protects, and as a bridge for the other server groups.

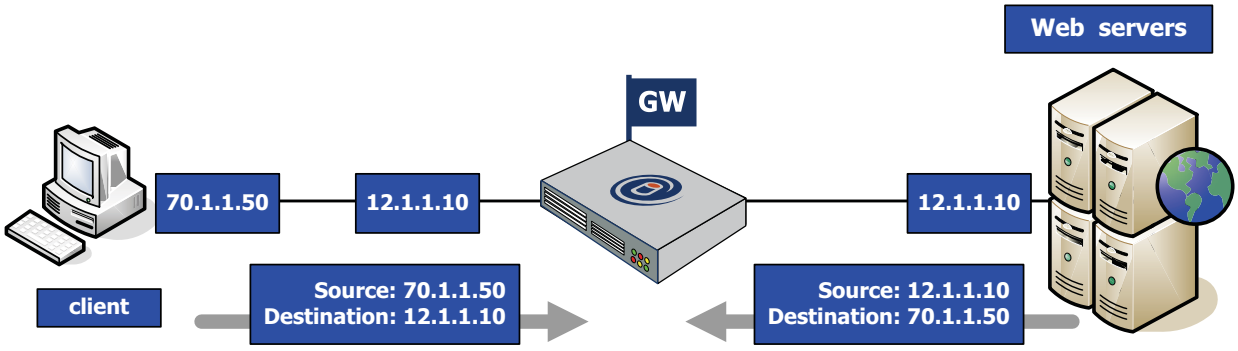


Figure 3 Transparent Reverse Proxy Deployment

The client begins the session by sending packets to the server's IP address (12.1.1.10). The SecureSphere gateway intercepts connections destined for the server, inspects them and forwards them on to the server.

The server sees the connections as coming from the client's IP address (70.1.1.50) and replies to that address. The return connection passes through the SecureSphere gateway, which inspects them and forwards them on to the client.

For information on configuring a SecureSphere gateway in Transparent Reverse Proxy, see Configuring Transparent Reverse Proxy on page 102.

Transparent Reverse Proxy - Selected Web Servers

In the deployment depicted in Figure 4, the SecureSphere gateway acts as a bridge, protecting all the servers (the two Web servers and the database server), but for one of the Web servers, the SecureSphere gateway also acts as a Transparent Reverse Proxy.

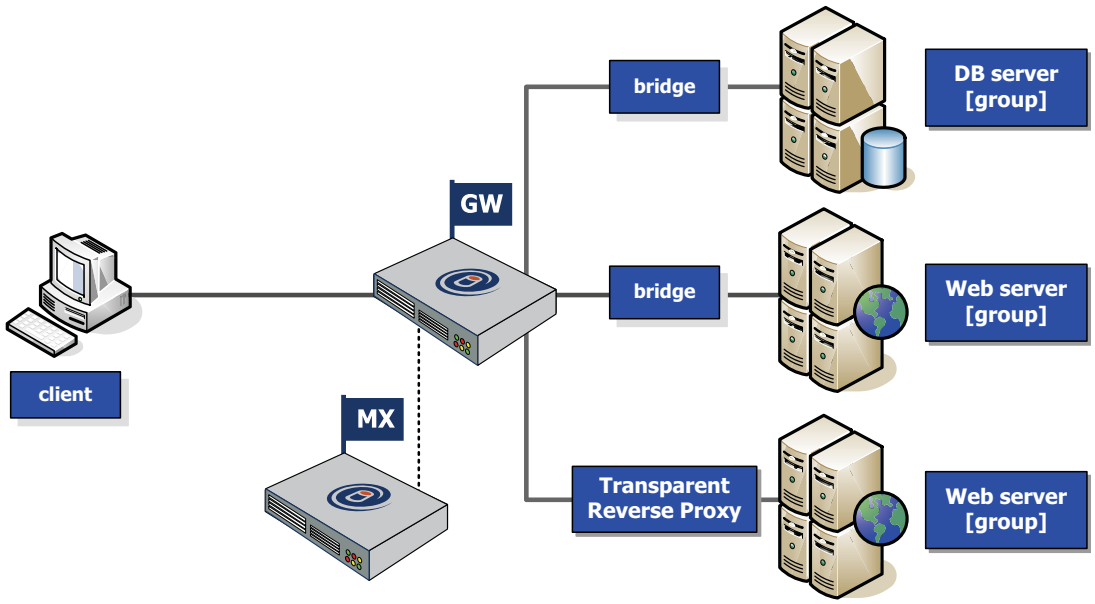


Figure 4 Transparent Reverse Proxy - Selected Web Servers

Non-Transparent Reverse Proxy Overview

There are two kinds of non-Transparent Reverse Proxy: Kernel Reverse Proxy (KRP) and Apache Reverse Proxy (ARP). These can be deployed on a SecureSphere gateway as follows:

- Kernel Reverse Proxy only
- Apache Reverse Proxy only
- Kernel Reverse Proxy and Apache Kernel Reverse Proxy together on the same gateway, where the ARP is deployed between the KRP and the Web server.

In non-Transparent Reverse Proxy mode, **c**lients connect to the IP address of the SecureSphere gateway, which acts as a Reverse Proxy for the Web servers it protects. In contrast to transparent deployments, in non-transparent deployments the SecureSphere gateway is visible to both client and server, while the client and server are not directly visible to each other.

The Web server groups are specified in the SecureSphere GUI (in the **Reverse Proxy** section of the **Definitions** tab of the server group (**Main** > **Setup** > **Sites**). The SecureSphere gateway does not act as a bridge. The Non-Transparent Reverse Proxy listens on the specified ports and ignores all other traffic.

Among the advantages of non-Transparent Reverse Proxies are:

- SSL off-loading: the ability to terminate SSL sessions, reducing the load on the server
- the ability to sign and encrypt cookies
- the ability to protect web servers located in multiple subnets, not necessarily close to each other or to the gateway

Some of the advantages of Kernel Reverse Proxy mode are:

- improved proxy functionality (connection termination, including SSL termination)
- improved proxy performance



Note: In Non-Transparent Reverse Proxy deployments, if the SecureSphere gateway fails, the Web server becomes unreachable, so High Availability is usually implemented to maintain connectivity. For more information, see Chapter 16, Gateway High Availability.

Kernel Reverse Proxy (KRP)

In a Kernel Reverse Proxy deployment, the client begins the session by sending packets to the SecureSphere gateway's inbound IP address. The SecureSphere gateway inspects the packets and, based on the rules, opens a second connection to the server, changing the packet's source IP address to the SecureSphere gateway's outbound IP address and the destination IP address to the real IP address of the server.

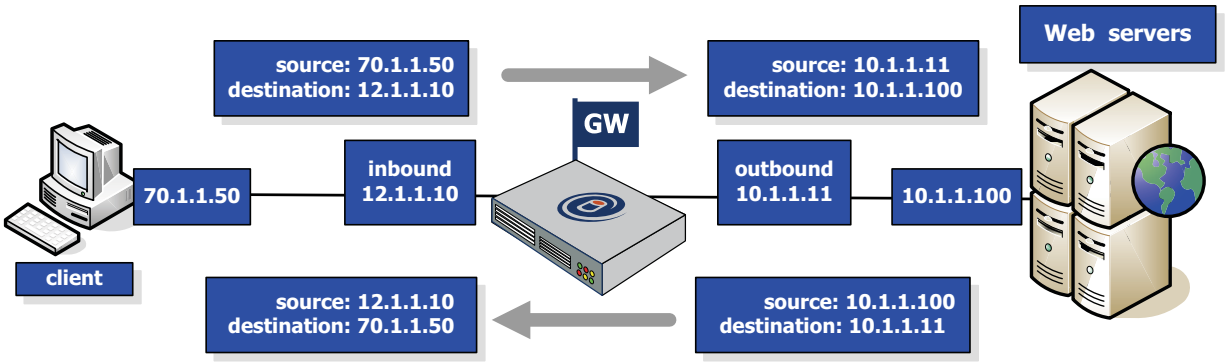


Figure 5 Non-Transparent Reverse Proxy Deployment

The server sends the return packets to the SecureSphere gateway, which inspects the packets and forwards them to the client, changing the source IP address to the SecureSphere gateway's inbound IP addresses, and the destination IP address to that of the client.

From the client's point of view, the server is the SecureSphere gateway's inbound IP address. From the server's point-of-view, the client is the gateway's outbound IP address.



Note: In KRP mode, the maximum length of a POST request without multi-parts is 2MB.

The SecureSphere gateway does not act as a bridge. The Kernel Reverse Proxy listens on the specified ports and ignores all other traffic.

The following sections describe a number of possible non-Transparent Reverse Proxy deployments.

- Kernel Reverse Proxy ("One Arm") on page 33
- Apache Reverse Proxy (ARP) on page 33
- Apache and Kernel Reverse Proxy on the Same Gateway on page 33
- Reverse Proxy with Load Balancer on page 34

Kernel Reverse Proxy ("One Arm")

A "one arm" Kernel Reverse Proxy deployment is one where the inbound and outbound interfaces are the same. This configuration simplifies routing.

Apache Reverse Proxy (ARP)

In contrast to a Kernel Reverse Proxy, the Apache Reverse Proxy runs in user space. Otherwise it is similar to the Kernel Reverse Proxy.

In this case too, the SecureSphere gateway does not act as a bridge. The Apache Reverse Proxy listens on the specified ports and ignores all other traffic.

Apache and Kernel Reverse Proxy on the Same Gateway

SecureSphere's Kernel Reverse Proxy has the advantage of speed and efficiency, but with some limitations such as the capability to rewrite full body content or to directly work with external authentication processes (SSO). In most scenarios these capabilities are not required. When they are required, they can be implemented by combing SecureSphere's Kernel Reverse Proxy with an Apache Reverse proxy running in user space on the same SecureSphere gateway.

When Apache Reverse Proxy and Kernel Reverse Proxy are implemented together, the Kernel Reverse Proxy redirects matching traffic (based on URl and/or hostname) to the Apache Reverse Proxy, which manipulates the session as required and communicates with the backend server. Return traffic follows the opposite route.

In the configuration shown in Figure 6, the client connects to the SecureSphere gateway, and the packets pass through both the SecureSphere Kernel Reverse Proxy (KRP) and the Apache Reverse Proxy (ARP).

Altogether there are three connections:

- client <-> Kernel Reverse Proxy
- Kernel Reverse Proxy <-> Apache Reverse Proxy
- Apache Reverse Proxy <-> backend Web server

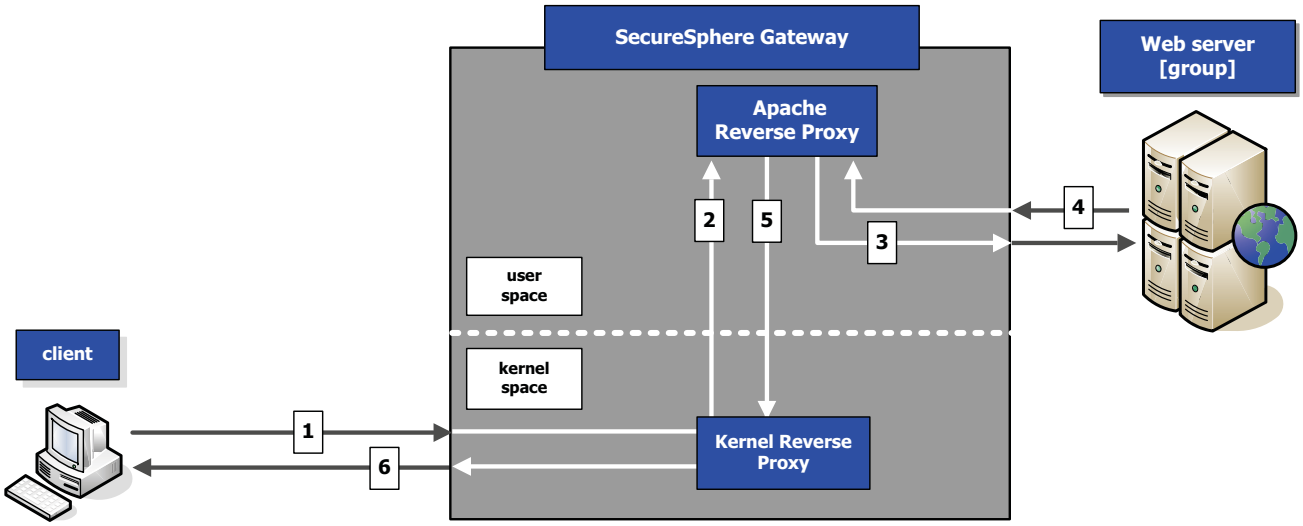


Figure 6 Inline Mode - Apache and Kernel Reverse Proxies

1. The client connects to the SecureSphere gateway's Kernel Reverse Proxy.
2. The Kernel Reverse Proxy inspects the packets and, based on the rules, opens a second connection to the Apache Reverse Proxy, running in user mode on the same SecureSphere gateway.
3. The Apache Reverse Proxy opens a third connection to the Web server.
4. The Web server sends the response to the Apache Reverse Proxy.
5. The Apache Reverse Proxy sends the response to the Kernel Reverse Proxy.
6. The Kernel Reverse Proxy inspects the response and sends it to the client.

For information on configuring a SecureSphere gateway as a Kernel Reverse Proxy and an Apache Reverse Proxy, see Configuring Kernel Reverse Proxy and Apache Reverse Proxy on the Same Gateway on page 117.

Reverse Proxy with Load Balancer

Load Balancers provide a number of advantages:

- High Availability — If one of the SecureSphere gateways fails, the Load Balancer will direct traffic to one of the other gateways.
- Increased Bandwidth — Since the processing load is shared among SecureSphere gateways, more total bandwidth is available.

Both Kernel Reverse Proxy and Apache Reverse Proxy can be implemented with Load Balancers.

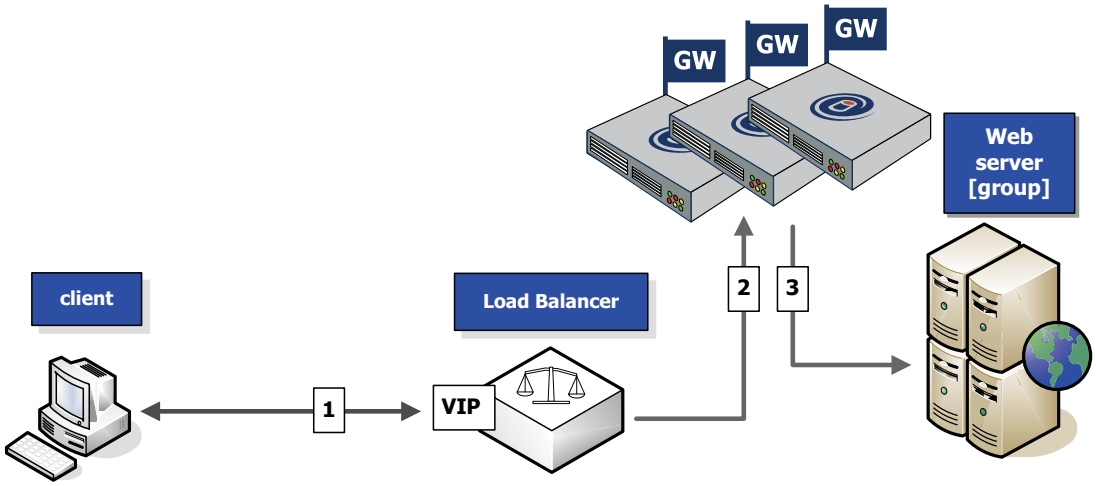


Figure 7 Inline Mode - Reverse Proxy with Load Balancer

1. The client connects to the external VIP (**V**irtual **IP**) address of the Load Balancer.
2. The Load Balancer opens a connection to a Reverse Proxy on one of the SecureSphere gateways.
3. The Reverse Proxy inspects the packets and, based on the rules, sends the connection to one of the Web servers.

Return traffic follows the opposite path.

Features Available in the Each Deployment Mode

Table lists some of the SecureSphere features for which the deployment mode affects the feature's availability. Note that sniffing deployments do not support proxies.

Some SecureSphere Features for which the Deployment Mode Affects the Feature's Availability

SecureSphere feature	Transparent Bridge	Sniffing	Reverse Proxy Modes		
			Transparent RP	Kernel RP (Non- Transparent)	Apache RP (Non- Transparent)
Inspect TCP handshake	✓	✓	✓	✓	✓
Normalize traffic (decode encoded content, such as URL-encoded or UTF-encoded content)	✓	✓	✓	✓	✓
Decrypt and inspect SSL (either interface to a FIPS-compliant HSM or store an encrypted copy of the SSL key)	✓	✓	✓	✓	✓
HTTP / SQL protocol conformance	✓	✓	✓	✓	✓
Session / cookie protection	✓	✓	✓	✓	✓
Input validation (white list)	✓	✓	✓	✓	✓
Attack detection (black list, including application, network, Web server and OS attacks)	✓	✓	✓	✓	✓
Correlated attack validation	✓	✓	✓	✓	✓
Block attacks	✓	✓[1]	✓	✓	✓
Block data leaks (inspect outgoing traffic for sensitive data such as SSN, credit card numbers, CVV numbers and data matching custom signatures)	✓	✘[1]	✓	✓	✓
Rewrite content	✘	✘	✓	✓	✓
Application level auditing (record complete HTTP request and server response code)	✓	✓	✓	✓	✓
Ignore IP Group (Server Groups)	✓	✓	✘	✘	✘
Application user tracking	✓	✓	✓	✓	✓

Some SecureSphere Features for which the Deployment Mode Affects the Feature's Availability

SecureSphere feature	Transparent Bridge	Sniffing	Reverse Proxy Modes		
			Transparent RP	Kernel RP (Non- Transparent)	Apache RP (Non- Transparent)
Firewall and Network Protocol Violation Policies enforced	✓	✗	✗	✗	✗
Redirect client to an error page	✓	✗[1]	✓	✓	✓

1. A SecureSphere gateway in sniffing mode cannot send an error page or block a connection. Instead, it sends a TCP reset to the server. The client sees a timeout message.

Guidelines

This section describes a number of practical guidelines of which administrators should be aware.

Gateways

The following guidelines apply to SecureSphere gateways:

- The number of server groups per Gateway should not exceed 30.

Management Servers

The following guidelines apply to SecureSphere Management Servers:

- The number of SSL certificates uploaded to a Management Server should not exceed 40K (key size 1024).
- The number of server groups per Gateway should not exceed 100.
- The number of Gateways per Management Server should not exceed 15.

Remote Agents

The following guidelines apply to SecureSphere Remote Agents:

- The number of Remote Agents per SecureSphere Gateway should not exceed 20.

CHAPTER 3

Platforms and Installation

This chapter describes the installation and configuration for SecureSphere appliances, and includes:

- Preparing the Appliance on page 41
- Installing the SecureSphere Software on page 42
- After Installing the SecureSphere Software on page 49

Forward Compatibility

In the past, Gateways and MXs had to be the same version in order for the MX to manage the Gateway.

Beginning with SecureSphere version 9.5, this is no longer the case. SecureSphere MXs are forward compatible with SecureSphere Gateways version 9.5 and higher. For example, a version 9.5 Gateway can be managed by a SecureSphere version 9.0 Patch 1 MX (but not by a pre-version 9.0 Patch 1 MX).

This means that when upgrading from SecureSphere version 9.0 or higher, you should upgrade the Gateways first and then upgrade the MX. This results in significantly reduced downtime during the upgrade process.

If, however, you are upgrading from SecureSphere versions prior to 9.0, you should follow the previous scenario: upgrade the MX first and then upgrade the MX.



Note:

- The MX must be version 9.0 Patch 1 or higher.
- This feature is not available for Onebox.
- If the MX and the Gateway are different SecureSphere versions, features added to SecureSphere after the version of the MX are not available. For example, a version 9.5 Gateway feature cannot be configured on a version 9.0 MX. The feature cannot be used until the MX is also upgraded.

Preparing the Appliance

Before configuring the SecureSphere software, you should open the required ports on firewalls in the network. For more information, see Configuring Firewall Ports on page 387.

Additionally, it is recommended that you provide an uninterrupted power source (UPS) for the appliance.

Installing the SecureSphere Software

The appliance is shipped from the factory with SecureSphere already installed on it. You can install a different version of SecureSphere on the appliance, from either the network or from a USB device, by following these instructions.

This section contains the following information:

- G Series Appliances (Except G2 and G2-2) on page 42
- G2 and G2-2 Appliances on page 44
- X and M Series Appliances on page 46
- Creating a Bootable USB Device Containing the Installation Image on page 47

G Series Appliances (Except G2 and G2-2)

Installation Monitoring

Before you begin, connect either a serial or VGA device. The factory-installed default is VGA.

For information about connecting a serial console, see Connecting to the G Series Appliance Using a Serial Console on page 43.

Installing From The Network

For information on how to install the latest version of the appliance software over the network, see Appendix A, Installing SecureSphere From the Network.

After installing the deployment program according to these instructions, you need to boot the appliance from the network. When the appliance boots, you will be prompted to press <F12> to boot from the network.

When the appliance tries to boot from the network, it will try both of the on-board interfaces, one after the other. Make sure you connect the cable to one of the appliance's defined Management Interfaces.

Installing From USB

To install from a USB device:

1. If there is a disk in the CD drive, remove it.
2. Turn off the appliance.
3. Plug a USB flash drive with the SecureSphere recovery image into the appliance USB port.
4. Boot the appliance and press the F2 key to enter the BIOS.
5. Go to **Boot Options**.
6. Set **Boot Option #1** to **CD**.
7. Set **Boot Option #2** to **RAID**.
8. Set **Boot Option #3** to **GE**.
9. Set **Boot Option #4** to **ERI Shell**.
10. Set **USB Boot Priority** to **Enabled**.
11. Save and exit the BIOS.
12. Turn off the appliance.
13. Plug a USB device with the SecureSphere recovery image into the appliance USB port.
14. Connect to the appliance using keyboard and VGA or serial monitor.

    For information about connecting a serial console, see Connecting to the G2 or G2-2 Appliance Using a Serial Console on page 45.
15. Turn the appliance on.
16. After the appliance boots, select either the second or the third installation option.

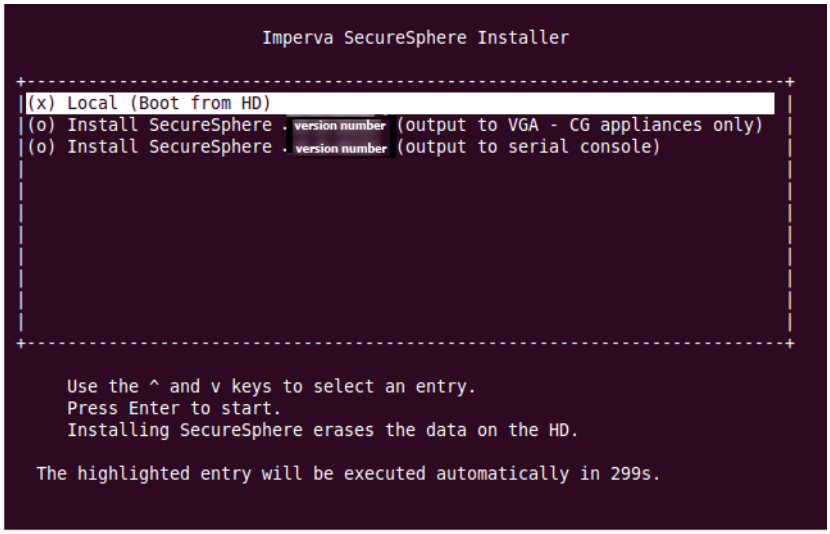


Figure 1 Installing from USB

17. Remove the USB key after the installation is complete.

Note: If you do not remove the USB key, you will be unable to use SecureSphere when the appliance is rebooted.

Connecting to the G Series Appliance Using a Serial Console

Note: This section is not relevant to G2 and G2-2 appliances. See Installation Monitoring on page 44 for information about commenting a serial device to these appliances.

To connect to the appliance using a serial console:

1. Connect a computer or a terminal to the serial port on the gateway using a serial cable. If you are using a program such as Hyperterminal™, configure the serial console settings as follows:

Serial Console Settings

Setting	Value
baud rate	38400
data bits	8
parity	none
stop bits	1
flow control	none
terminal emulation	VT-100 or VT-UTF8

Note: Some terminal emulators correctly interpret the Backspace key to delete the previous character from the stream sent to the application as well as from the displayed text, while others send a control sequence, so that the stream the application sees is different from the displayed text. You should determine the behavior of your terminal emulator before using the Backspace key.
In Hypterterminal, you can avoid this problem by using the DEL option.

G2 and G2-2 Appliances

The appliance is shipped from the factory with SecureSphere already installed on it. You can install a different version of SecureSphere on the appliance, from a USB device, a CD or the network, by following these instructions.

Installation Monitoring

Before you begin, connect either a serial or VGA device. The factory-installed default is VGA.

For information about connecting a serial console, see Connecting to the G2 or G2-2 Appliance Using a Serial Console on page 45.

Installing From The Network

For information on how to install the latest version of the appliance software over the network, see Appendix A, Installing SecureSphere From the Network.

eth2 is the interface used for network installations.

To boot from the network:

1. Boot the appliance and press the DEL key to enter the BIOS.
2. Go to **Advanced Bios Features**.
3. Change **First Boot Device** to **LAN3**. This is the factory-installed default.
4. Save and exit the BIOS.
5. Connect the network to eth2.
6. Reboot the appliance.
7. Press F12.

   If you do not press F12, the installation will be from the second boot device.
8. Follow the instructions on the screen.

Installing From USB

To install from a USB device:

1. If there is a disk in the CD drive, remove it.
2. Turn off the appliance.
3. Plug a USB flash drive with the SecureSphere recovery image into the appliance USB port.
4. Boot the appliance and press the F2 key to enter the BIOS.
5. Go to **Advanced Bios Features**.
6. Change **USB Flash Disk Type** to **HDD**.
7. Change **First Boot device** to **USB-HDD**.
8. Change **Second Boot Device** to **USB-HDD**.
9. Change **Third Boot Device** to **USB-HDD**.
10. Set **Boot Other Device** to **Disabled**.
11. Set **USB emulation** to **HDD**.
12. Save and exit the BIOS.
13. Turn off the appliance.
14. Connect to the appliance using keyboard and VGA or serial monitor.

    For information about connecting a serial console, see Connecting to the G2 or G2-2 Appliance Using a Serial Console on page 45.
15. Turn the appliance on.
16. After the appliance boots, select either the second or the third installation option.

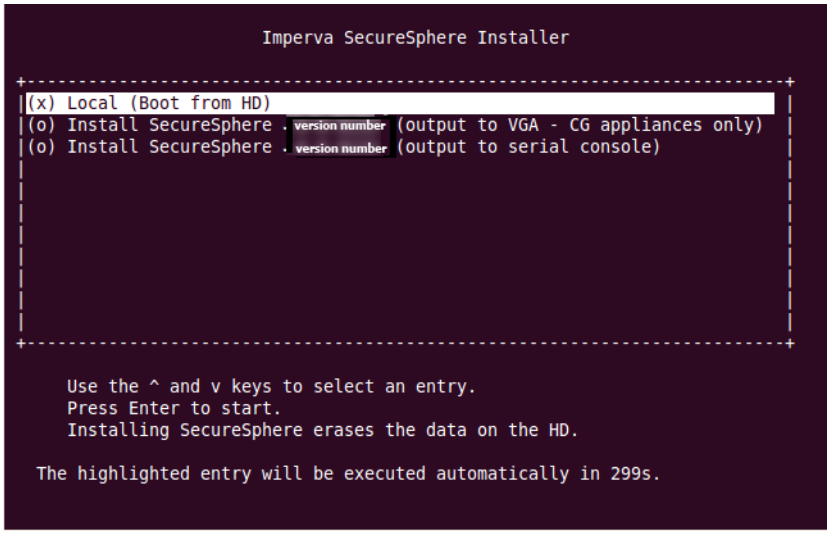


Figure 2 Installing from USB

17. Remove the USB key after the installation is complete.



Note: If you do not remove the USB key, you will be unable to use SecureSphere when the appliance is rebooted.

18. Reboot the appliance.

Installing Using an External CD Drive

To connect an external CD drive:

1. Connect the CD to the appliance's USB.
2. Boot the appliance and press the DEL key to enter the BIOS.
3. Go to Advanced Bios Features.
4. Change **Second Boot device** to **USB-CDROM**.
5. Save and exit the BIOS.

Connecting to the G2 or G2-2 Appliance Using a Serial Console

To connect to the appliance using a serial console:

1. Boot the appliance and press the DEL key to enter the BIOS.
2. Go to **Advanced Bios Features**.
3. Set **Console Redirection** to **Enabled**.
4. Set **Baud Rate** to **38400**.
5. Set **Agent Connect via** to **NULL**.
6. Set **Agent wait time (sec)** to **3**.
7. Set **Agent after boot** to **Enabled**.
8. Save and exit the BIOS.

X and M Series Appliances

Connecting to a X or M Series Appliance Using a Serial Console

To connect to the appliance using a serial console:

1. Connect a computer or a terminal to the serial port on the appliance using a serial cable. If you are using a program such as Hyperterminal™, configure the serial console settings as follows:

Serial Console Settings

Setting	Value
baud rate	38400
data bits	8
parity	none
stop bits	1
flow control	none
terminal emulation	VT-100 or VT-UTF8 (supports colors)



Note: Some terminal emulators correctly interpret the Backspace key to delete the previous character from the stream sent to the application as well as from the displayed text, while others send a control sequence, so that the stream the application sees is different from the displayed text. You should determine the behavior of your terminal emulator before using the Backspace key.
In Hypterterminal, you can avoid this problem by using the DEL option or Ctrl-H (delete character).

Installing From USB

To install from a USB device:

1. Turn off the appliance.
2. Plug a USB device with the SecureSphere recovery image into the appliance USB port.
3. Connect to the appliance using a serial console (see Creating a Bootable USB Device Containing the Installation Image on page 47).
4. Power on the appliance.
5. After the appliance boots, select the first or the third installation option.

   The second option is relevant only for G appliances, or for LOM configurations.

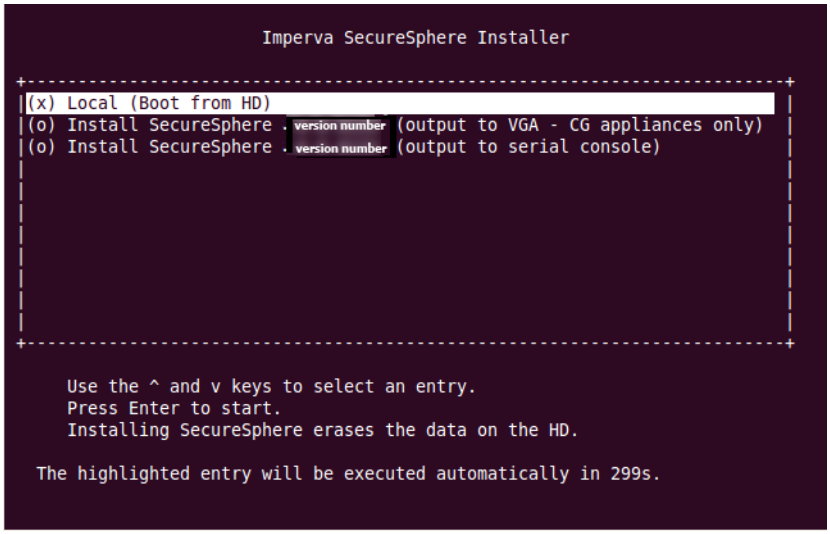


Figure 3 Installing from USB

Installing From The Network

For information on how to install the latest version of the appliance software over the network, see Appendix A, Installing SecureSphere From the Network.

After installing the deployment program according to these instructions, you need to boot the appliance from the network. When the appliance boots, you will be prompted to press **L** to boot from the network.

When the appliance tries to boot from the network, it will try both of the on-board interfaces, one after the other. Connect the cable to the default management interface and optionally, to the LAN management interface.

Creating a Bootable USB Device Containing the Installation Image

To install SecureSphere from a USB device, you must first create an image of the installation file on the device. You will need the following:

- a USB device (for example, a disk on key) with a capacity of at least 4GB.

  Note: All data on the device will be erased, so back up the data before starting this procedure.

- access to the Internet

To create a bootable USB device:

1. Download the image of the USB file from the Imperva FTP site.

	Location
32 bit	`/Downloads/SecureSphere_Setup/v9.5/32Bit/USB/`
64 bit	`/Downloads/SecureSphere_Setup/v9.5/64Bit/USB/`

2. Download and install the Image Writer for Windows executable file from the following URL:
   http://launchpad.net/win32-image-writer/
3. Attach your USB device to your computer.
4. Start the Image Writer for Windows application.

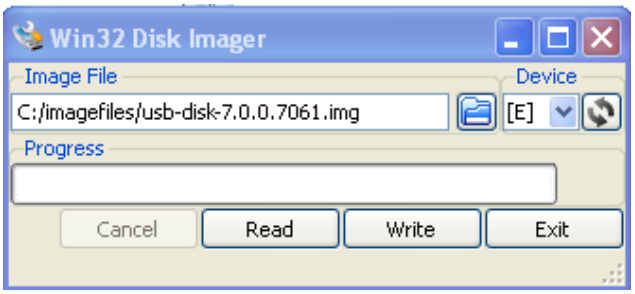


Figure 4 Win32 Disk Imager window

5. Under **Device**, select your USB device.
6. If your USB device is not listed under **Device**, refresh the list by clicking the icon to its right.
7. If the image file you downloaded in step 1 is not listed under **Image File**, browse to the image file you downloaded in step 1.
8. Confirm that **Image File** and **Device** are correct.



Note: Make sure you are not formatting the wrong disk, for example, your hard drive.

9. Click **Write**.

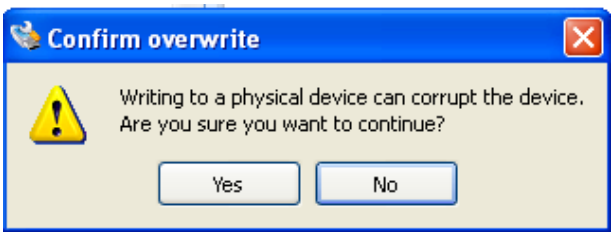


Figure 5 Confirm overwrite window

10. In the **Confirm Overwrite** window, click **Yes**.
11. After the image has been copied to the USB device, you can use it to install SecureSphere.

After Installing the SecureSphere Software

Management Servers

Connecting to the Management Server

To configure SecureSphere using the GUI, connect to the Management Server by pointing your browser to https://<IP address>:8083, where <IP address> is the IP address of the management port on the MX.



Note: For more information, see the ***Quick Start Guide*** for your MX appliance.

MySQL Users

This section is relevant when using one of the following SecureSphere features with a MySQL database:

- DB Data Classification
- Assessment
- Credentials Verification
- Test Connection

You must download and install an MySQL driver on the SecureSphere Management Server (MX) before using these features.

To download and install the MySQL driver:

1. Go to `http://dev.mysql.com/Downloads/Connector-J/mysql-connector-java-5.1.7.zip` to download the following file: `mysql-connector-java-5.1.7.zip`.
2. Click **No thanks, just take me to the downloads!**
3. After downloading the file, extract the `mysql-connector-java-5.1.7-bin.jar` file from it.
4. Copy the extracted file (`mysql-connector-java-5.1.7-bin.jar`) to the following directory on the MX:

   `/opt/SecureSphere/server/SecureSphere/jakarta-tomcat-secsph/webapps/SecureSphere/WEB-INF/lib`

5. Restart the MX using the following command:

```
impctl server restart
```

CHAPTER 4

Configuring SecureSphere

This chapter describes the initial installation procedure for SecureSphere, and also the additional configuration steps required before SecureSphere can become operational, including:

- Initial Configuration on page 51
- IPv6 on page 52
- SecureSphere Users on page 56
- Appliance OS on page 57
- Gateway/Management Server Appliance Initial Configuration on page 59
- Configuring SecureSphere Using the Command Line Tools on page 60
- Configuring a Management Server on page 69
- Configuring a Gateway on page 71
- Managing Remote Agents on page 76
- Configuring a Data Assessment Server (DAS) on page 81
- Configuring the Platform on page 84
- Configuring SecureSphere Routes on page 99
- Configuring Transparent Reverse Proxy on page 102
- Configuring Kernel Reverse Proxy on page 103
- Configuring Apache Reverse Proxy on page 110
- Configuring Kernel Reverse Proxy and Apache Reverse Proxy on the Same Gateway on page 117
- Switching Deployments on page 118

Initial Configuration

Instructions for the physical configuration of the SecureSphere appliance are provided in the ***Quick Start Guide*** packaged with the appliance.

During the First Time Login, the administrator is required to define the following:

- the password for the appliance's **`root`** user
- the password for the **`secure`** user (the SecureSphere administrative "superuser")
- for Management Servers, for the **`system`** user (the password for the internal SecureSphere database)
- additional OS users (CLI users), who are able to run a restricted set of OS commands (see CLI Users on page 57)
- the appliance's management interface IP address (in CIDR format)

  This interface is usually used for managing SecureSphere gateways, so that the interface used to manage the management server is distinct from the interface the management server uses to communicate with the gateways.
- the appliance's management interface (NIC) for out-of-band management
- the appliance's hostname
- the appliance's default gateway
- the appliance's operation mode (sniffing, bridge, *etc.*)
- for virtual appliances, the appliance model number
- the time zone

Once these parameters have been defined, the administrator defines the additional configuration parameters required to make the SecureSphere operational. The additional parameters which must be defined depend on the appliance's operational mode (management server, sniffing gateway, bridge, *etc.*).



Note: A SecureSphere management server is also known as an "MX".

IPv6

This section describes IPv6 support, which is implemented in SecureSphere beginning with Version 9.0.



Note: Additional information regarding IPv6 support is given in the “Basic Configuration” chapter of the ***SecureSphere User Guide***.

SecureSphere Features Which Support IPv6

SecureSphere supports IPv6 in the following SecureSphere features:

- WAF
- MX-Gateway communications
- VRRP
- communications with external systems which support IPv6 (see External Systems on page 55)

Overview

IPV6 Address Formats

IPv6 addresses are 128 bits long and are written in eight groups of four hexadecimal digits separated by colons, for example, **2001:0db8:85a3:0000:0000:8a2e:0370:7334**. The hexadecimal digits are case-insensitive.

An IPv6 address can be abbreviated according to following rules:

- Leading zeroes within a 16-bit value may be omitted. For example, the address **fe80:0000:0000:0000:0202:b3ff:fe1e:8329** may be written as **fe80:0:0:0:202:b3ff:fe1e:8329**.
- A single occurrence of any number of consecutive groups of zeroes within an address may be replaced by a double colon. For example, **fe80:0:0:0:202:b3ff:fe1e:8329** becomes **fe80::202:b3ff:fe1e:8329**.

So the same IPv6 address can be represented in several different ways. For example, the following are all equivalent:

2001:db8:0:0:1:0:0:1	2001:0db8::1:0:0:1
2001:0db8:0:0:1:0:0:1	2001:db8:0:0:1::1
2001:db8::1:0:0:1	2001:db8:0000:0:1::1
2001:db8::0:1:0:0:1	2001:DB8:0:0:1::1

Whenever an IPv6 address is entered into SecureSphere, after it is saved it is displayed in the “long” format. For an example, when the IPv6 address as "**2001:DB8::**" is entered in the GUI and saved, it is then displayed as "**2001:0DB8:0000:0000:0000:0000:0000:0000**", except in **`impcfg`**, where one of the short forms (not necessarily the shortest) of the address is used.



Note: SecureSphere is able to recognize the equivalence of these different forms of the same IPv6 address, except in certain cases where the IPv6 address is treated as a character string, for example, in lookup datasets and in ThreatRadar.

CIDR Notation

Classless Inter-Domain Routing (CIDR) notation explicitly specifies the number of bits in an IP address denoting the network, in contrast to the netmask notation which indirectly specifies the number of bits. For example, a netmask of **255.255.255.0** indicates (for IPv4 addresses) a network in which the first 24 bits of an IP address denote the network. In CIDR notation, one simply writes "/24" after the IP address (for example, **123.124.125.126/24**). The advantages of CIDR notation over the netmask notation are simplicity and scalability from IPv4 to IPv6.

The IP address/netmask notation is no longer permitted for both IPv4 and IPv6 addresses. Instead, CIDR notation is used both in the SecureSphere GUI and **impcfg**.



Note: CIDR notation is used only when specifying a network or when configuring a local IP address where it is necessary to specify the subnet. CIDR is not to be used when specifying a remote IP address, for example, that of an NTP server or a DNS server, or when defining the Management Server of a SecureSphere Gateway.
When **impcfg** requires that CIDR notation be used, it specifies so in the prompt, for example, “Enter IP address/CIDR”. If “CIDR” is not specified in the prompt, it must not be entered.

IPv4 / IPv6 Dual Stack

The source and destination IP addresses of an IP packet must both be either IPv4 or IPv6. It is not possible for one of the addresses to be IPv4 and the other to be IPv6. The solution is to assign to a device both an IPv4 and an IPv6 address, so that the device can communicate on both protocols.

So, for example, if an MX manages both IPv4 and IPv6 Gateways, the MX’s management or LAN interface (whichever one the Gateways communicate with) must have both an IPv4 and an IPv6 address.

At various points in the SecureSphere GUI and in **impcfg**, users are prevented from trying to define an IPv4-IPv6 connection.

SecureSphere MX and Gateway

SecureSphere Management Servers and Gateways can have IPv6 addresses. An MX can simultaneously manage Gateways with IPv4 addresses together with Gateways with IPv6 addresses, if the MX’s management interface or its LAN interface has both an IPv4 and an IPv6 address.

A SecureSphere GUI user can point his browser to an IPv6 SecureSphere MX.

IPv6 is supported for Gateway syslog, MX syslog and MX-Gateway communications.

Hostnames

When entering a hostname, the “:” is not allowed.

IPv6 in impcfg and impctl

The following points are relevant specifically to **impcfg** and **impctl**.

1. **impcfg** and **impctl** accept both IPv4 and IPv6 addresses, for example for DNS and NTP servers. In all cases where IPv6 is supported (note the exceptions below) the user can assign to the same entity:
   - both IPv4 and IPv6 addresses
   - an IPv4 address only
   - an IPv6 address only

   An IPv6 address can be specified for external servers (for example, DNS or NTP), only if either the appliance’s management or LAN interface has an IPv6 address.
2. When **impcfg** asks the user to enter an IP address for a management or LAN interface, it allows the user to enter either an IPv4 or IPv6 address, and then asks the user if he wants to enter an address of the other type (so, for example, if he enters an IPv4 address, he will be asked if he wants to enter an IPv6 address, and he can either enter one or not enter one).

3. As noted above, network masks have been replaced by CIDR notations for both IPv4 and IPv6 addresses. While in the past, users were asked to enter an IP address/netmask pair (for local IP addresses and network addresses - for example, when specifying a static route - and for sniffing mode blocking masks), users are now asked (for both IPv4 and IPv6 addresses) to enter an IP address in CIDR notation.

   For example, instead of entering an IP address of **144.234.123.0** and a netmask of **255.255.255.0**, the user enters only one field: **144.234.123.0/24**.



Note: CIDR notation is used only when specifying a network or when configuring a local IP address where it is necessary to specify the subnet. CIDR is not to be used when specifying a remote IP address, for example, that of an NTP server or a DNS server, or when defining the Management Server of a SecureSphere Gateway.
When **impcfg** requires that CIDR notation be used, it specifies so in the prompt, for example, “Enter IP address/CIDR”. If “CIDR” is not specified in the prompt, it must not be entered.

4. Link-local addresses (**fe80::/10**) are not supported and cannot be entered anywhere in **impcfg**.
5. Default gateway - this is unchanged (for both IPv4 and IPv6), that is, the user is not required to specify the device (interface).
6. VRRP routes (KRP and legacy, that is, pre version 7.0, Remote Agents) - **impcfg** tries to deduce the device (interface) from the aliases, and if it cannot, it asks the user.
7. **portguard** supports IPv6. Access to the appliance’s link-local addresses is blocked.
8. When configuring a SecureSphere Gateway, the user will not be able to specify an IPv6 management interface if the MX management and LAN interfaces both have only IPv4 addresses. If the Gateway's management or LAN interface has both IPv4 and IPv6 addresses, then the communication will depend on whether the user specifies the IPv4 or IPv6 address as the management interface on the Gateway.
9. **ping6** is not blocked for SecureSphere appliances (as **ping** is).

Exceptions

The following exceptions apply:

1. IPv6 addresses for Remote Agent and SecureSphere Agent for DB2 z/OS listeners are not supported in this version. Users will not be able to enter IPv6 addresses for them in **impcfg**. This means that a SecureSphere Gateway which listens to a Remote Agent or a SecureSphere Agent for DB2 z/OS must have an IPv4 address.
2. IPv6 is not supported in MX-HA.
3. IPv6 VRRP static routes are not supported.
4. IPv6 DHCP is not supported (DAS).
5. The following commands have been deprecated:
   - **impctl vrrp gateway show**
   - **impctl vrrp gateway config**

External Systems

SecureSphere MX can communicate over IPv6 with the external systems listed below:

External System	
HTTP Proxy	**Admin** > **System Definitions** > **External HTTP Settings**
SMTP	SMTP servers with IPv6 addresses.
SNMP	SNMP nodes with IPv6 addresses.
LDAP endpoint access	LDAP servers with IPv6 addresses.
LDAP authentication	
FTP archive	Archiving audit files to an IPv6 archive via FTP.
SCP archive	Archiving audit files to an IPv6 archive via SCP.
Remote Access to Infra to IPv6	Enables remote access to servers, to run shell scripts remotely.

SecureSphere MX **cannot** communicate over IPv6 with the external systems listed below:

External System		Reason
Oracle Server	**Admin** > **System Definitions** > **External Systems**	
MSSQL Server		
MySQL Server		This product is not yet IPv6 compliant.
SQL		
HTTP/HTTPS archive	**Admin** > **System Definitions** > **Action Interfaces**	
BMC Remedy		This product is not yet IPv6 compliant.

SecureSphere Users

The Different SecureSphere Users

Several users are created for a SecureSphere appliance, each for a different purpose. Each of these users has its own password.

SecureSphere Users and Passwords

SecureSphere User	Description
CLI Users	
root	This is the all-powerful superuser of the appliance's Linux-based OS. This user is created automatically by SecureSphere when it is installed. **Note:** You cannot login to the appliance as root over SSH. To administer the appliance remotely, login as a CLI user other than **root** and **secure** over SSH and enter the **admin** command. For more information, see CLI Users on page 57. For information about changing this user's password, see Configuring the Platform on page 84.
secure	This is the SecureSphere administrative superuser, who has complete read-write access to all SecureSphere components, including configuring the appliance with the command line application **impcfg**. This user is created automatically by SecureSphere when it is installed. This user is not the same as the internal SecureSphere "admin" GUI user (see below). **Note:** You cannot login to the appliance as **secure** over SSH. For information about changing this user's password, see Configuring a Management Server on page 69 and Configuring a Gateway on page 71.
system	This is the user of the internal SecureSphere database, and is required only on a SecureSphere Management Server. This user is created automatically by SecureSphere when it is installed. For information about changing this user's password, see Configuring a Management Server on page 69.
Other CLI users	These are OS users, at least one of whom must be defined during the First Time Login, who are allowed to run a restricted number of OS commands in order to administer the appliance. The sessions of other CLI users (but not of **root** and **secure**) are logged to the file **/var/log/secure** to enforce accountability. For information on logging these sessions to **syslog**, see the Imperva Knowledge Base. For more information, see CLI Users on page 57.
SecureSphere GUI users	
These are the users of the SecureSphere GUI, some of whom are defined within SecureSphere as administrators. One user ("admin") is pre-defined and has complete read-write privileges, including that of defining other SecureSphere GUI administrators and users. For more information, see Chapter 9, Users and Permissions.	

Appliance OS

The appliance OS is based on a “hardened” version of Linux.

CLI Users

At least one other CLI user (in additon to the CLI users created automatically by SecureSphere: **root**, **secure** and **system**) must be defined during the First Time Login. You can define any number of additional CLI users using **impcfg**.

Other CLI users are allowed to run only the following OS commands:

- **impcfg** - This command opens a shell session as the **secure** user.
- **passwd**
- **admin** - This command opens a shell session as the **root** user.

All commands issued by CLI users (except **root** and **secure**) are logged to the file **/var/log/secure**. For information on logging these sessions to **syslog**, see the Imperva Knowledge Base.



Note:

- It is possible to to connect to the appliance as a CLI user over the SFTP protocol (for example, using WinSCP) but not over SCP.
- By default, you cannot connect to the appliance as **root** or **secure** over SSH. To login as **root**, you must first connect as a CLI user and use the **admin** command. However, you can specify an IP address from which user **root** is allowed to login over SSH using the following command:
  impctl hardening config --root-source-ip-exception=<IP address>

Authentication Failure

CLI users other than **root** and **secure** who fail authentication 6 times are locked out for 30 minutes. An administrator can release the lock before this time using **impcfg** (see Manage User on page 95).

Passwords

The minimum length for SecureSphere passwords (**root** and **secure** and other CLI users) is 7 characters, and the maximum length is 255 characters. Passwords may consist only of alphabetic characters, numeric characters, and special characters.

The password for **system** must be less than 30 characters long.



Warning: It is of the utmost importance that all these passwords be “strong” (that is, difficult to guess), and that they be treated with discretion.

Passwords for other CLI users (not those of **root** and **secure**) expire after 90 days, and users are warned, starting 7 days before the expiration date, that they must change their password. After the 90 day period, users have an additional 7 day grace period to change their password. If they do not change their password during that time they are locked out until an administrator releases the lock (see Manage User on page 95).

After changing their passwords, users must wait at least 7 days before changing their passwords again.

Passwords are hashed using SHA-2.

Timeout

Shell sessions for all users are timed out after 15 minutes.

Date Changes

Whenever the system date is changed, a log event is sent to syslog, so that administrators are notified. Locally, the events are stored in **`/var/log/secure`**.

Gateway/Management Server Appliance Initial Configuration

When configuring an appliance for the first time (the first-time login), the **impcfg** wizard guides you through a question and answer procedure. After confirming that all the information is correct, this initial configuration is applied to the system components using the **impctl** application. This process takes between 45 minutes and 1 hour for a Management Server, where a database must be created and initialized. On a Gateway the process takes between 10-15 minutes.



Note:
- The instructions for the initial configuration (first-time login) are given in the appliance's Quick Start Guide, which is packaged with the appliance.
- If you configure a DNS client during the first-time login, make sure you specify the IP address of a real DNS server.

Additional configuration is performed using the menu-driven **impcfg** command line application. For more information, see Configuring SecureSphere Using the Command Line Tools on page 60.

If you run the first-time configuration script after the appliance has already been configured, the previous configuration is overwritten.

First-Time Login (Configuration)

The First-Time Login is usually via the console port. Once the appliance has a management IP address, further interactions can be via the console, or SSH. Make sure that SSH communication is possible for remote appliance configuration (port 22 on the firewall must be open).



Note: You cannot login to the appliance as **root**, **secure**, or **system** over SSH.

For more information on which firewall ports must be open, see Configuring Firewall Ports on page 387.

If you are configuring a Management Server and a Gateway, configure the Management Server first. The reason is that when a Gateway is configured, the Management Server must be running and reachable. If not, the gateway must be restarted when the Management Server is alive and reachable. Check the Gateway status from the Gateway Management screen (Figure 3 on page 71).

After the First-Time Login, you can configure SecureSphere using the GUI by pointing the browser to **https://<IP address of MX>:8083**.

Registering a Gateway

In order to establish the relationship between a SecureSphere Gateway and its Management Server, you must register the Gateway to the Management Server. Registration is part of the First Time Login procedure for the gateway, during which you will be asked to specify the IP address of the Management Server.



Note: You cannot specify a CIDR address for a SecureSphere Gateway's Management Server. For more information about when CIDR can be used, see CIDR Notation on page 53.

You can unregister a Gateway from one Management Server and register it to a different Management Server using the **impcfg** application. For more information, see Configuring a Gateway on page 71.

Configuring SecureSphere Using the Command Line Tools

There are two command line interface (CLI) tools with which you can configure SecureSphere on the management server and gateways:

- **`impcfg`** is a menu-based configuration tool that can be used to configure both the Management Server and the Gateway.

  `impcfg` is described in this section.
- **`impctl`** is a lower level configuration tool. **`impcfg`** runs **`impctl`** on the SecureSphere appliance to deploy the configuration which the administrator defines in **`impcfg`**.

  `impctl` is described in Appendix E, Command Line Interface.

Command Line Tools and MX-HA

Changing MX Properties in an MX-HA Environment



Note: For more information about MX-HA, see Chapter 17, Management Server High Availability (MX-HA).

In an MX-HA environent, it is not possible to perform any of the following appliance-level actions on the MX using the command line tools **`impcfg`** and **`impctl`**:

- change the MX's network properties, for example, its IP addresses, interfaces (devices), *etc.*
- change the MX's hostname
- change MX passwords (**`system`** and **`secure`** - see SecureSphere Users on page 56 for more information)



Warning: **`impcfg`** and **`impctl`** will let you make these changes, and you will not receive an error message, but the MX and the MX-HA environment may become inoperational and you will have to re-install MX-HA.

If you need to perform any of the above changes, you must uninstall MX-HA on both the primary and secondary MXs, make the changes and then reinstall MX-HA.

Stopping and Starting the MX in an MX-HA Environment

The correct way start and stop the MX in an MX-HA environment is by using the following commands:

```
impctl server ha start
impctl server ha stop
```



Warning: Do not use **`impcfg`** or **`impctl`** to start and stop the MX as you would in a non-MX-HA environment (as described in Configuring a Management Server on page 69). Use only the above commands.

impcfg

By default, there are two ways to run **impcfg**:

- Log in to the appliance remotely over SSH as another CLI user and run **impcfg**.
- Log in to the appliance remotely over SSH as another CLI user and use the **admin** command, and then run **impcfg**.

Note: Some terminal emulators correctly interpret the Backspace key to delete the previous character from the stream sent to the application as well as from the displayed text, while others send a control sequence, so that the stream the application sees is different from the displayed text. You should determine the behavior of your terminal emulator before using the Backspace key.
In Hypterterminal, you can avoid this problem by using the DEL option.

Top Screen

The first screen displayed is the **Top** screen, shown in Figure 1.

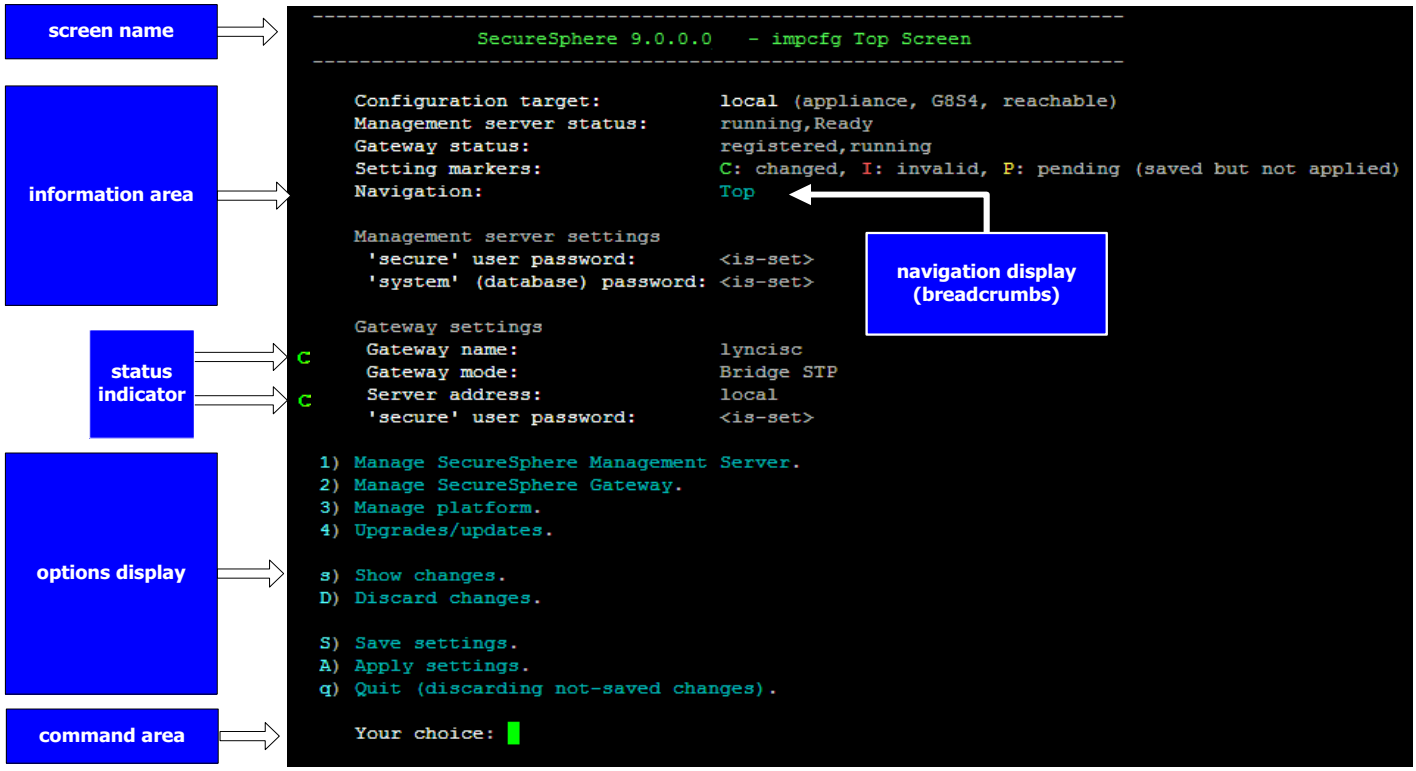


Figure 1 impcfg Top Screen

Table lists the components of all **impcfg** screens.

impcfg Screen Components

Screen Component	color	Description
screen name	green	The name of the screen and the SecureSphere version number.

impcfg Screen Components (continued)

Screen Component	color	Description
information area		Displays information about the gateway or management server being configured. Entries in the information area may be shown with the following status indicators: • I (red I) = invalid setting • C (green C) = changed (unsaved setting) • P (yellow P) = pending (saved but not applied)
status indicator		
options display	**blue**	A list of command numbers with their meanings. In addition to the numbered commands, you can choose one of the following: • e = End this level • j = Jump up to a previous level • t = Jump up to the top level • q = Quit (discarding non-saved changes) • S = Save settings • A = Apply settings • C = Confirm action
command area	**green**	The area in which the administrator enters commands and their arguments. Often, the default value [in square brackets] is displayed here.
navigation display	**blue**	"Breadcrumbs" indicating which screen is currently being displayed and the path followed to reach it. In the example shown in Figure 3, we are in the Gateway Management screen, so the path is **Top -> Gateway**.

In the **Top** screen, you can configure SecureSphere by entering the number of one of the displayed options, as listed below.

Top Screen Configuration Options

Option	Name	Description
The numbers of these options change, depending on the appliance's configuration	Manage Secure Sphere Server	Configure and manage a SecureSphere management server. For more information, see Configuring a Management Server on page 69.
	Manage SecureSphere Gateway	Configure and manage a SecureSphere gateway. For more information, see Configuring a Gateway on page 71.
	Manage SecureSphere DAS	Configure and manage a SecureSphere Data Assessment Server (DAS). For more information, see Configuring a Data Assessment Server (DAS) on page 81.
	Manage platform	Configure and manage an appliance. For more information, see Configuring the Platform on page 84.
	Upgrades / updates	This option is reserved for future use.
	Reconfigure as OneBox (immediate)	Reconfigure the DAS as a Onebox. For more information, see Reconfiguring the DAS as a Onebox on page 83

Top Screen Configuration Options (continued)

Option	Name	Description
s	Show changes	Display a list of changes made in this session.
D	Discard changes	Discard all the changes made in this session.
S	Save settings	Save all the configuration changes made in this session without applying them.
A	Apply settings	This option performs the following: • Saves all the configuration changes made in this session. • Applies all pending configuration changes (including changes made in previous sessions which were saved but not applied) to the management server and/or gateways as appropriate. Except for those **`impcfg`** menu items which explicitly indicate that they are executed immediately, all changes take effect only when they are applied using this option.

impcfg Functionality Map

Table shows the complete **`impcfg`** functionality.



Note: (I) means immediate activation, that is, the command is executed and, if relevant, the SecureSphere database is updated immediately.

impcfg Functionality Map

Top Screen Menu	Level 1 menu	Level 2 menu	Level 3 menu	For more information, see
Manage SecureSphere Server	Deactivate server			Configuring a Management Server on page 69
	Restart server **(I)**			
	Stop server **(I)**			
	Change management password			
	Change database password			
	Deactivate server			

impcfg Functionality Map (continued)

Top Screen Menu	Level 1 menu	Level 2 menu	Level 3 menu	For more information, see
Manage SecureSphere Gateway	Perform actions (start, stop, etc.)	Unregister gateway **(I)**		Configuring a Gateway on page 71
		Soft gateway restart **(I)**		
		Hard gateway restart (teardown/ prepare resources) **(I)**		
		Stop gateway **(I)**		
		Refresh gateway status **(I)**		
Manage SecureSphere Gateway *(continued)*	Change gateway name			
	Change server address /password			
	Change operation mode	Sniffing		Configuring a Gateway as a Sniffing Gateway on page 75 **Note:** The management server must be running when you execute this command.
		Bridge STP		Configuring a Gateway as a Bridge on page 73
		Bridge IMPVHA		
		Reverse Proxy Apache		Configuring Apache Reverse Proxy on page 110
		Reverse Proxy Kernel		Configuring Kernel Reverse Proxy on page 103
	Manage hardware security modules (HSM)	enable nCipher HSM		Hardware Security Modules (HSM) on page 400
		enable SafeNet HSM		

impcfg Functionality Map (continued)

Top Screen Menu	Level 1 menu	Level 2 menu	Level 3 menu	For more information, see
	Manage remote agents	Add a legacy (pre 7.0) agent		Managing Remote Agents on page 76
		Modify a legacy (pre 7.0) agent		
		Delete a legacy (pre 7.0) agent		
		Add agent listener		
		Delete agent listener		
		Add z/OS agent listener(s)		
		Delete z/OS agent listener		
		Manage remote agent routes		
Manage SecureSphere Gateway *(continued)*	Manage interfaces and routes *(for a bridge)*	Create bridge		Configuring a Gateway as a Bridge on page 73
		Delete bridge		
		Toggle STP on a bridge		
		Toggle High Availability on a Bridge		
	Manage interfaces and routes *(for a sniffing gateway)*	Set sniffing interface(s)		Configuring a Gateway as a Sniffing Gateway on page 75
		Set blocking interface		
		Add/modify blocking mask		
		Delete blocking mask		

impcfg Functionality Map (continued)

Top Screen Menu	Level 1 menu	Level 2 menu	Level 3 menu	For more information, see
	Manage interfaces and routes *(for a Kernel Reverse Proxy)*	Add alias		Configuring Kernel Reverse Proxy on page 103
		Modify Alias		
		Delete Alias		
		Enable high availability		
		Manage reverse proxy (kernel) routes		
	Manage interfaces and routes *(for an Apache Reverse Proxy)*	Add alias		Configuring Apache Reverse Proxy on page 110
		Modify Alias		
		Delete Alias		
		Enable high availability		
		Manage reverse proxy (kernel) routes		
Manage SecureSphere DAS	Deactivate server			Configuring a Data Assessment Server (DAS) on page 81
	Restart server **(I)**			
	Stop server **(I)**			
	Change management password			
	Change database password			
	Deactivate server			

impcfg Functionality Map (continued)

Top Screen Menu	Level 1 menu	Level 2 menu	Level 3 menu	For more information, see
Manage platform	Manage network	Management interface	Change device	Management Interface on page 86
			Change IP address	
			Change netmask	
			Locate device **(I)**	
		LAN interface	Change device	LAN Interface on page 88
			Change IP address	
			Change netmask	
			Locate device **(I)**	
		Default gateway		Default Gateway on page 89
		Static routes	Add route	Static Routes on page 89
			Delete route	
		Name Resolution (DNS client)	Enable DNS client	Name Resolution (DNS client) on page 90
			Set domain	
			Set search list	
			Set name servers	
		Locate network devices		Locate Network Devices on page 91
	Manage time	Add time server		Time Servers on page 92
		Delete time server		
	Manage users			Users Management on page 92
	Manage hostname			Hostname Management on page 97
	Manage bootloader password			Bootloader Password Management on page 98
	Reboot the appliance **(I)**			Configuring the Platform on page 84
	Shutdown the appliance **(I)**			Configuring the Platform on page 84

impcfg Functionality Map (continued)

Top Screen Menu	Level 1 menu	Level 2 menu	Level 3 menu	For more information, see
Upgrade / updates				This option is reserved for future use.

Configuring a Management Server

You can:

- activate/deactivate the Management Server
- start/stop/reactivate the Management Server
- change management and database passwords

Note: The management and database passwords cannot be changed form the OS command line.

To configure the Management Server:

1. In the **Top** Screen, select option **1) Manage SecureSphere Server**.
   The **Server Management** screen is displayed.

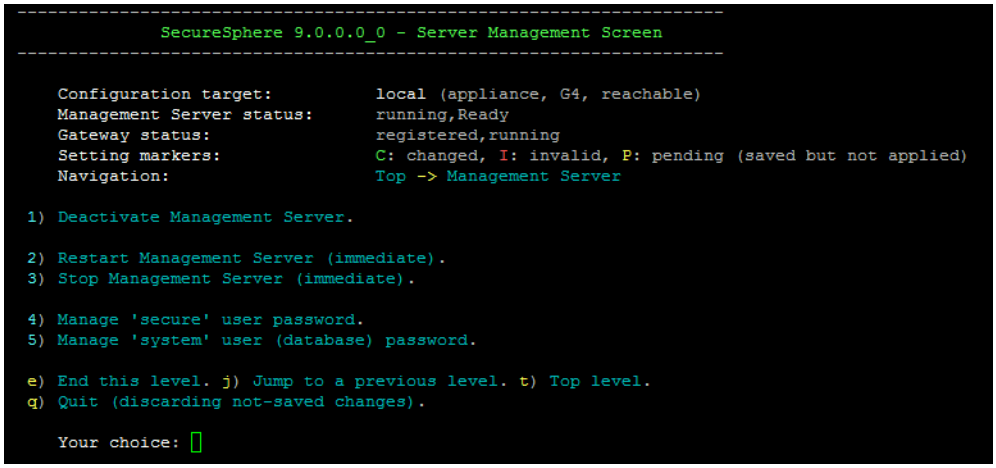


Figure 2 Server Management screen

2. Select one of the following options, as listed below.

Appliance Management Configuration Options

Option	Name	Description
1	Deactivate Management Server	Stop the Management Server and do not restart it when the appliance boots. This would be done, for example, when converting a Onebox to a gateway (which will be managed by another Management Server).
	Activate Management Server	Start the Management Server the next time the appliance boots. This would be done, for example, when converting a gateway to a Onebox.
2	Restart Management Server (immediate)	Stop and then start the Management Server.
3	Stop Management Server (immediate)	Stop the Management Server.

Appliance Management Configuration Options (continued)

Option	Name	Description
4	Manage ‘secure’ user password	Change the password of the **secure** user. **Note:** This option restarts the Management Server and is not supported in Management Server High Availability deployments. For more information about Management Server High Availability, see Chapter 17, Management Server High Availability (MX-HA). For more information about passwords, see SecureSphere Users on page 56.
5	Manage ‘system’ user (database) password	Change the password of the internal SecureSphere database. **Note:** This password must be less than 30 characters. **Note:** This option restarts the Management Server and is not supported in Management Server High Availability deployments. For more information about Management Server High Availability, see Chapter 17, Management Server High Availability (MX-HA). For more information about passwords, see SecureSphere Users on page 56.

Configuring a Gateway

You can:

- activate/deactivate, register/unregister, start/stop/reactivate the gateway
- change the gateway name, server address/password, and operation mode
- manage HSM, high availability, remote agents, and interfaces

To configure the gateway:

1. In the **Top** Screen, select option **2) Manage SecureSphere Gateway**. The **Gateway Management** Screen is displayed.

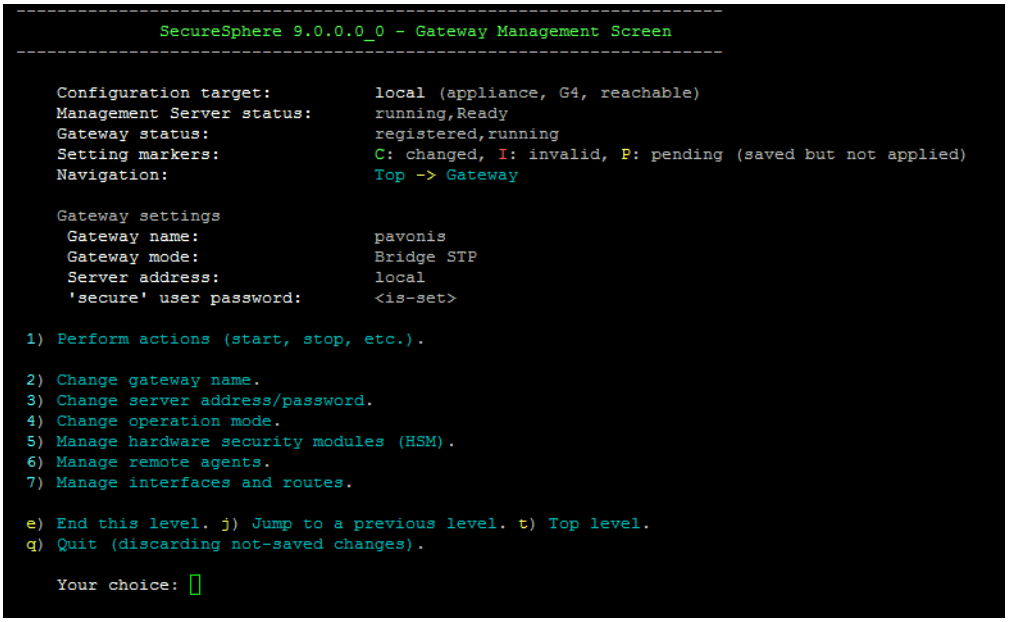


Figure 3 Gateway Management screen

2. Select one of the following options, as listed below.

Appliance Management Configuration Options

Option	Name	Description
1	Perform actions (start, stop, *etc.*)	Start, stop or unregister the gateway.
2	Change gateway name	Change the gateway's name. This option is used, for example, when a gateway is moved to another network.
3	Change server address/password	Specify a different Management Server for the gateway. This option is used, for example, when a gateway is moved to another network, and will be managed by a different Management Server. **Note:** You cannot specify a CIDR address for a Gateway's Management Server. For more information about when CIDR can be used, see CIDR Notation on page 53. When you apply this change, the gateway registers with the Management Server.

Appliance Management Configuration Options (continued)

Option	Name	Description
4	Change operation mode	Change the mode of the gateway to one of the following: • **sniffing**: For more information, see Configuring a Gateway as a Sniffing Gateway on page 75. • **bridge STP**: For more information, see Configuring a Gateway as a Bridge on page 73. • **bridge IMPVHA**: For more information, see Configuring a Gateway as a Bridge on page 73. • **Reverse Proxy Apache**: For more information, see Configuring Apache Reverse Proxy on page 110. • **Reverse Proxy Kernel**: For more information, see Configuring Kernel Reverse Proxy on page 103. **See also**: Chapter 2, Topologies and Deployment.
5	Manage hardware security modules (HSM)	For more information, see Hardware Security Modules (HSM) on page 400.
6	Manage remote agents	For more information, see Managing Remote Agents on page 76.
7	Manage interfaces and routes	For more information, see Configuring SecureSphere Routes on page 99.

Gateway Actions

You can:

- register/unregister the gateway
- restart the gateway (soft or hard restart)
- stop the gateway
- refresh the gateway's status

To perform gateway actions:

1. In the **Top** Screen, select option **2) Manage SecureSphere Gateway**.
2. In the **Gateway Management** screen, select **1) Perform actions (start, stop, etc.)**.

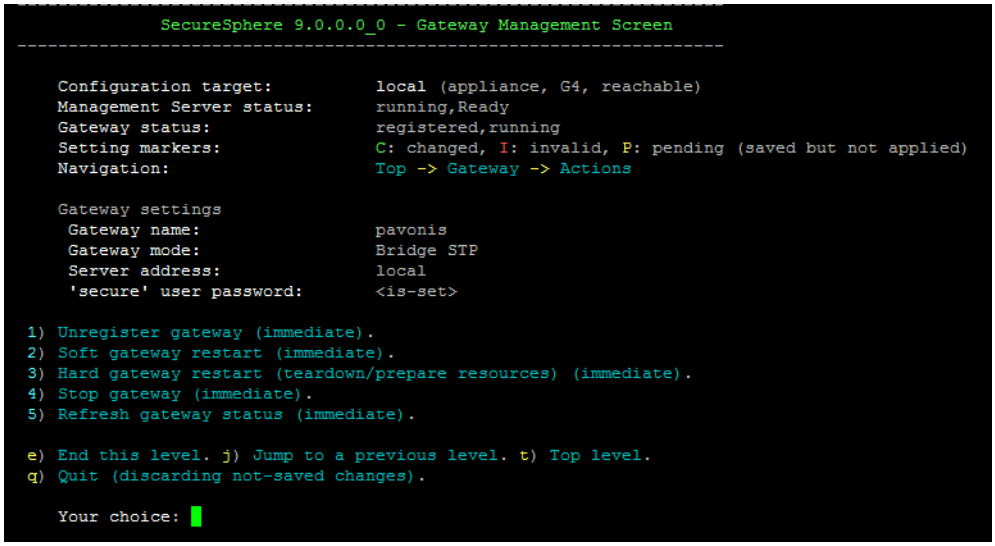


Figure 4 Gateway Actions screen

3. Select one of the following options, as listed below.

Gateway Actions Options

Option	Name	Description
1	Register / Unregister gateway (immediate)	Register or unregister the gateway from the management server.
2	Soft gateway restart (immediate)	
3	Hard gateway restart (immediate)	
4	Stop gateway (immediate)	
5	Refresh gateway status (immediate)	

Configuring a Gateway as a Bridge

To configure a gateway as a bridge:

1. In the **Gateway Management** screen (Figure 3 on page 71), select option **4) Change operation mode**.
2. From the list of operation modes (Figure 5), select one of the bridge modes:
   - **2) Bridge STP** or
   - **3) Bridge IMPVHA**.

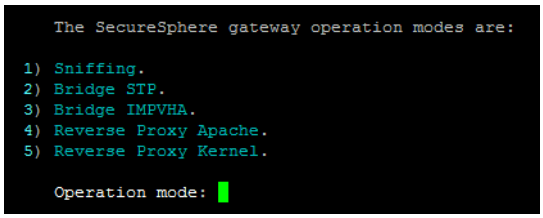


Figure 5 Gateway Operation Modes

Note: Bridge STP mode does not correctly pass Cisco PVST PDU packets. Use Bridge IMPVHA mode if you need to pass these packets.

3. In the **Gateway Management** screen (Figure 3 on page 71), select option **7) Manage interfaces and routes**.

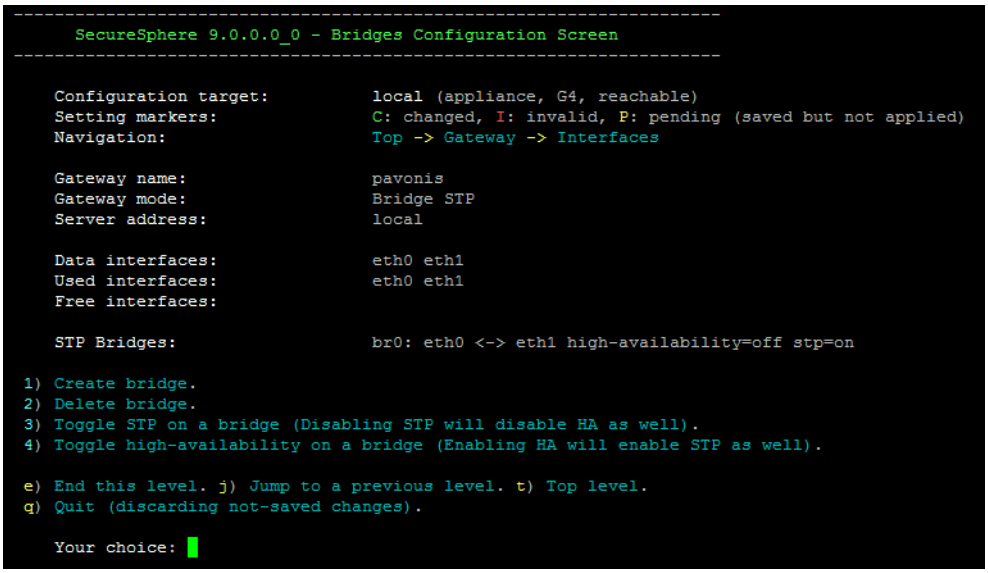


Figure 6 Bridges Configuration screen

4. In the **Bridges Configuration** screen, select one of the following options, as listed below.

Bridges Configuration Options

Option	Name	Description
1	Create bridge	Create a bridge on available interfaces.
2	Delete bridge	Delete an existing bridge.
3	Toggle STP on a bridge	Select an existing bridge and toggle STP on it. For more information, see Chapter 2, Topologies and Deployment.
4	Toggle High Availability on a Bridge	Select an existing bridge and toggle High Availability on it. **Note:** To enable High Availability on a bridge, you must enable STP on that bridge. For more information, see Chapter 16, Gateway High Availability.

Note:
- If the gateway is not in a High Availability deployment, it is recommended that the gateway be configured as Bridge IMPVHA with HA disabled.
- SecureSphere does not support jumbo packets.

Configuring a Gateway as a Sniffing Gateway

To configure a sniffing gateway:

1. In the **Gateway Management** screen (Figure 3 on page 71), select option **4) Change operation mode**.
2. From the list of operation modes (Figure 5), select **1) Sniffing**.



Warning: The management server must be running when you execute this command, otherwise the gateway will switch to bypass mode.

3. In the **Gateway Management** screen (Figure 3 on page 71), select option **7) Manage interfaces and routes**.

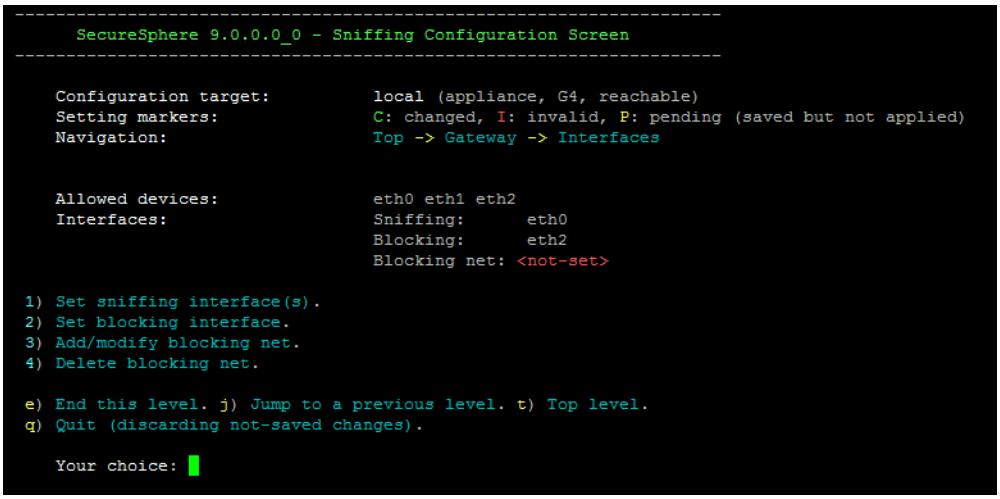


Figure 7 Sniffing Configuration screen

4. In the **Sniffing Configuration** screen, select one of the following options, as listed below.

Sniffing Configuration Options

Option	Name	Description
1	Set sniffing interface(s)	Specify the interface to be used for sniffing.
2	Set blocking interface	Specify the interface to be used for blocking, that is, the interface from which SecureSPhere sends RST packets.
3	Add/modify blocking mask	Specify the following for the blocking interface: • the blocking device (one of the interfaces) • the blocking interface IP address • the blocking interface IP mask
4	Delete blocking mask	Select the blocking mask to be deleted.

Managing Remote Agents

You can:

- add/modify/delete remote agents
- add and delete agent listeners
- add and delete SecureSphere Agent for DB z/OS listeners

SecureSphere Remote Agents, installed on the database server, provide visibility into database activity by monitoring all database communications and forwarding these communications, via a TCP or UDP tunnel, to a listener application configured on a SecureSphere gateway.

Note: Bridge and sniffing interfaces cannot be defined as TCP listener interfaces.

Usually, when a Remote Agent is installed and configured, it registers with the SecureSphere gateway. Upon successful registration, the gateway configures the Remote Agent with the listener port used for the tunnel.

For more information about Remote Agents, see ***SecureSphere User Guide***.

To manage remote agents:

1. In the **Gateway Management** screen (Figure 3 on page 71), select **7) Manage remote agents**. The **Remote Agents** Screen is displayed.

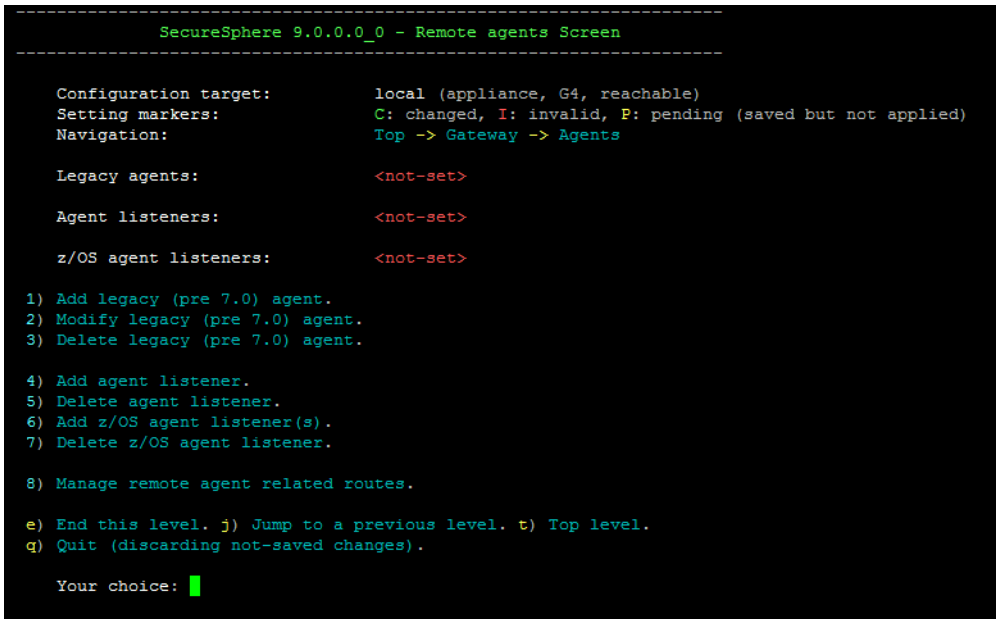


Figure 8 Remote Agent screen

2. Select one of the following options, as listed below.

Remote Agent Configuration Options

Option	Name	Description
1	Add a legacy (pre 7.0) agent	Add a pre-version 7.0 remote agent. For more information, see Adding a Legacy (pre-version 7.0) Remote Agent on page 77.

Remote Agent Configuration Options (continued)

Option	Name	Description
2	Modify a legacy (pre 7.0) agent	Modify a pre-version 7.0 remote agent. For more information, see Modifying a Legacy (pre-version 7.0) Remote Agent on page 78.
3	Delete a legacy (pre 7.0) agent	Delete a pre-version 7.0 remote agent. For more information, see Deleting a Legacy (pre-version 7.0) Remote Agent on page 78.
4	Add agent listener	Add a listener for a remote agent. This option is not relevant to SecureSphere Agent for DB2 z/OS. **Note:** A Remote Agent listener and a SecureSphere Agent for DB2 z/OS listener cannot be defined on the same port. **Note:** Bridge and sniffing interfaces cannot be defined as TCP listener interfaces. For more information, see Adding a Remote Agent Listener on page 78.
5	Delete agent listener	Delete a listener for a remote agent. This option is not relevant to SecureSphere Agent for DB2 z/OS. For more information, see Deleting a Remote Agent Listener on page 79.
6	Add z/OS agent listener(s)	Add a SecureSphere Agent for DB2 z/OS listener. **Note:** A Remote Agent listener and a SecureSphere Agent for DB2 z/OS listener cannot be defined on the same port. For more information, see Adding a SecureSphere Agent for DB2 z/OS Listener on page 79.
7	Delete z/OS agent listener	Delete a SecureSphere Agent for DB2 z/OS listener. For more information, see Deleting a SecureSphere Agent for DB2 z/OS Listener on page 79.
8	Manage remote-agent related routes	Manage remote agent routes. For more information, see Managing Remote Agent Related Routes on page 80.

Adding a Legacy (pre-version 7.0) Remote Agent

To add a legacy (pre-verson 7.0) agent:

1. Enter the remote agent name.
   This field corresponds to the **Agent Name** in the Agents Workbench.
2. Enter the remote agent ID.
3. Enter a description for the remote agent.

Modifying a Legacy (pre-version 7.0) Remote Agent

To modify a legacy (pre-verson 7.0) agent:

1. Select the remote agent from the displayed list.
2. Enter a new remote agent name.
   This field corresponds to the **Agent Name** in the Agents Workbench.
3. Enter a new remote agent ID.
4. Enter a new description for the remote agent.

Deleting a Legacy (pre-version 7.0) Remote Agent

To delete a legacy (pre-verson 7.0) agent:

1. Select the remote agent from the displayed list.
   The remote agent will be immediately deleted.

Adding a Remote Agent Listener

To add a Remote Agent listener:



Note:
- These parameters must also be specified in the Remote Agent configuration on the database server. For more information, see Remote Agent Management Console on page 146.
- You can define multiple listeners of both types (TCP and UDP) on a gateway, and you can direct different Remote Agents to different listeners.
- Bridge and sniffing interfaces cannot be defined as TCP listener interfaces.
- A Remote Agent listener and a SecureSphere Agent for DB2 z/OS listener cannot be defined on the same port.

1. Enter the listener protocol (TCP or UDP).

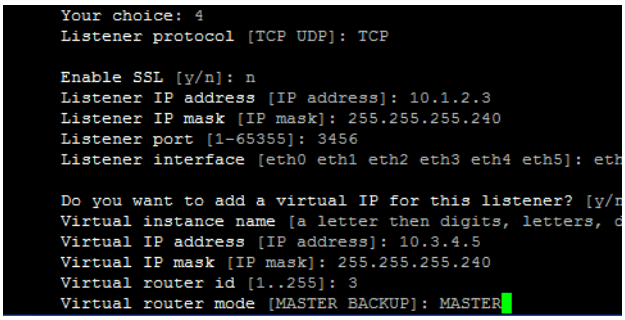


Figure 9 Remote Agent Listener

2. Select whether to use SSL.
3. Enter the listener IP address.



Note: Only IPv4 addresses are allowed for Remote Agent listeners.

4. Enter the listener network mask.
5. Enter the listener port.
6. Enter a Remote Agent listener interface.
7. Specify whether to add a virtual IP address for the listener.

If you choose to specify a virtual IP address, you will be asked to define some additional parameters:

- Virtual instance name
- Virtual IP address
- Virtual IP mask
- Virtual router id
- Virtual router mode

Deleting a Remote Agent Listener

To delete a Remote Agent listener:

1. Select the Remote Agent listener from the displayed list (by number).

   The Remote Agent listener will be immediately deleted.

Adding a SecureSphere Agent for DB2 z/OS Listener



Note:

- These parameters must also be specified in the SecureSphere Agent for DB2 z/OS configuration on the database server. For more information, see ***SecureSphere User Guide***.
- A Remote Agent listener and a SecureSphere Agent for DB2 z/OS listener cannot be defined on the same port.

1. Select the listener type.

```
   Your choice: 6

1) Data Receiver Listener Type.
2) Plan Provider Listener Type (configuration).

   Listener tunnel type [1..2]: 1
   Listener IP address [IP address]: 10.1.2.3
   Listener IP mask [IP mask]: 255.255.255.240
   Listener port [1-65355]: 2345
   Listener interface [eth0 eth1 eth2 eth3 eth4 eth5]: eth0

   You are now configuring Plan Provider Listener Type (configuration)
   Listener IP address [IP address]: 10.2.4.5
   Listener IP mask [IP mask]: 255.255.255.240
   Listener port [1-65355]: 3333
   Listener interface [eth0 eth1 eth2 eth3 eth4 eth5]: eth2
```

Figure 10 Remote Agent Listener Definition

Data Receiver listeners are for audit events, and messages sent from the SecureSphere Agent for DB2 z/OS to the SecureSPhere gateway.

Plan Provider listeners are for the policies, plans and messages sent between the gateway and the SecureSphere Agent for DB2 z/OS.

2. Enter the other parameters as requested.
3. You must define one listener of each type, so after you have defined the first listener, you will be asked to define the other listener as well (see Figure 10).

Deleting a SecureSphere Agent for DB2 z/OS Listener

To delete a SecureSphere Agent for DB2 z/OS listener:

1. Select the SecureSphere Agent for DB2 z/OS listener from the displayed list (by number).

   The SecureSphere Agent for DB2 z/OS listener will be immediately deleted.

Managing Remote Agent Related Routes

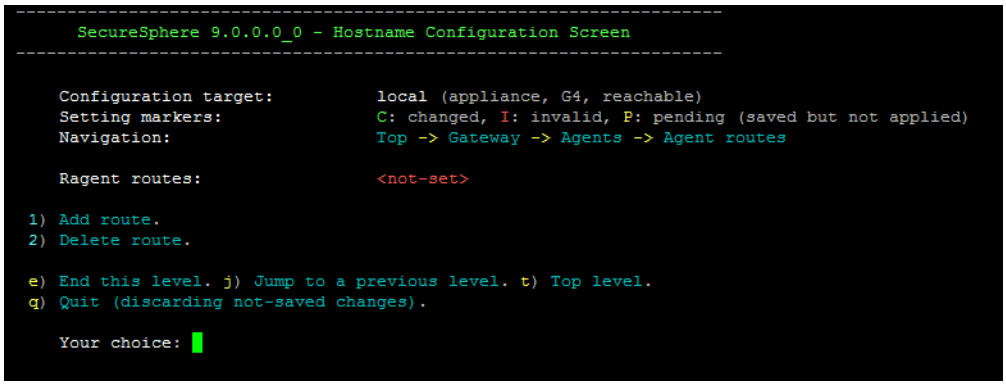


Figure 11 Remote Agent Routes Definition

1. From the Remote Agent Routes screen, select one of the following options, as listed below.

Static Routes Screen Configuration Options

Option	Name	Description
1	Add route	Add a remote agent route.
2	Delete route	Delete an existing remote agent route.

2. Enter the route parameters, as requested.

Configuring a Data Assessment Server (DAS)

For an appliance configured as a Data Assessment Server (DAS), you can:

- activate/deactivate the DAS
- start/stop/reactivate the DAS
- change management and DAS passwords
- reconfigure the DAS as a Onebox

Note: If the appliance has not been configured as a DAS, the DAS options are not available.

To configure the DAS:

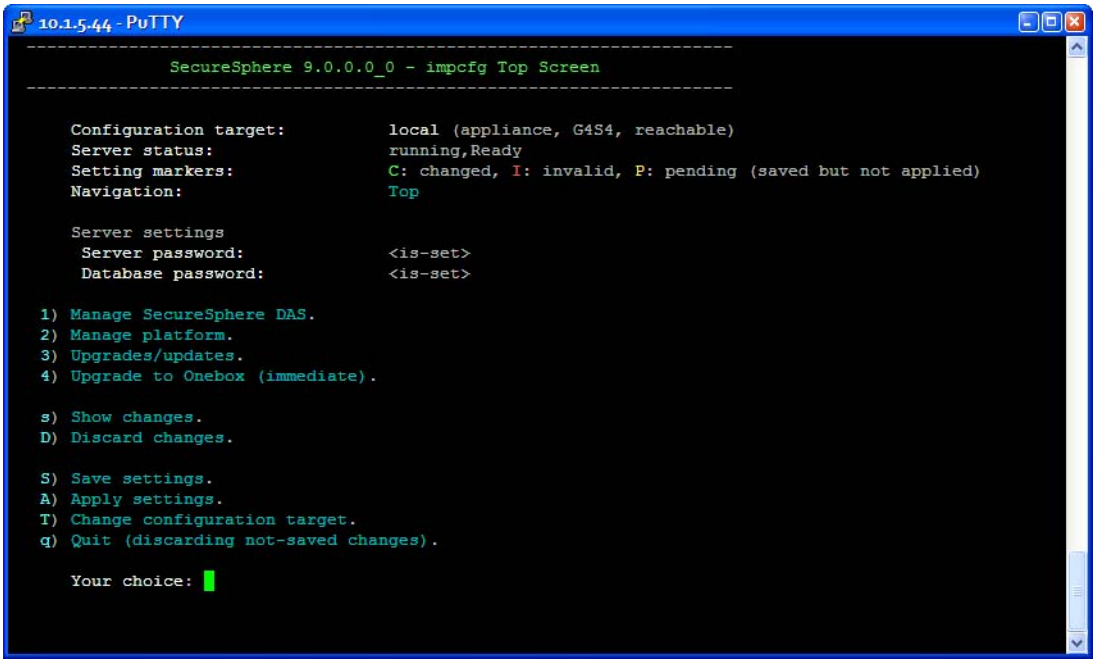


Figure 12 impcfg Top Screen (DAS)

1. In the **Top** Screen (Figure 12), select option **1) Manage SecureSphere DAS**.
   The **Gateway Management** Screen (Figure 13) is displayed.

Note: A DAS appliance can only discover vulnerabilities but cannot mitigate them.

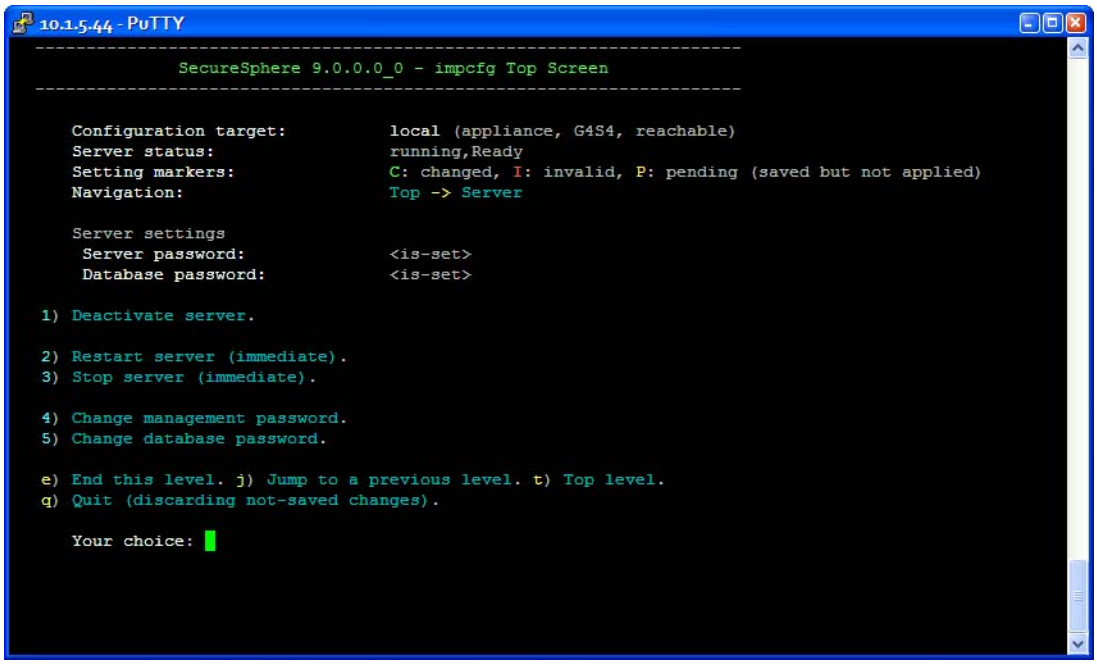


Figure 13 DAS Server Configuration screen

2. Select one of the following options, as listed below.

DAS Configuration Options

Option	Name	Description
1	Deactivate server	Stop the DAS and do not restart it when the appliance boots. This would be done, for example, when converting a DAS to a Onebox.
	Activate Server (immediate)	Start the DAS the next time the appliance boots. This would be done, for example, after a Onebox has been converted to a DAS.
2	Restart server (immediate)	Stop and then start the DAS.
3	Stop server (immediate)	Stop the DAS.
4	Change management password	Change the password of the **secure** user. For more information about passwords, see SecureSphere Users on page 56.
5	Change database password	Change the password of the internal SecureSphere database. For more information about passwords, see SecureSphere Users on page 56.

Reconfiguring the DAS as a Onebox

You can reconfigure a DAS as a Onebox.

To reconfigure the DAS as Onebox:

1. In the **Top** Screen, select option **4) Reconfigure as Onebox**. The **Reconfigure DAS to Onebox** Screen is displayed.

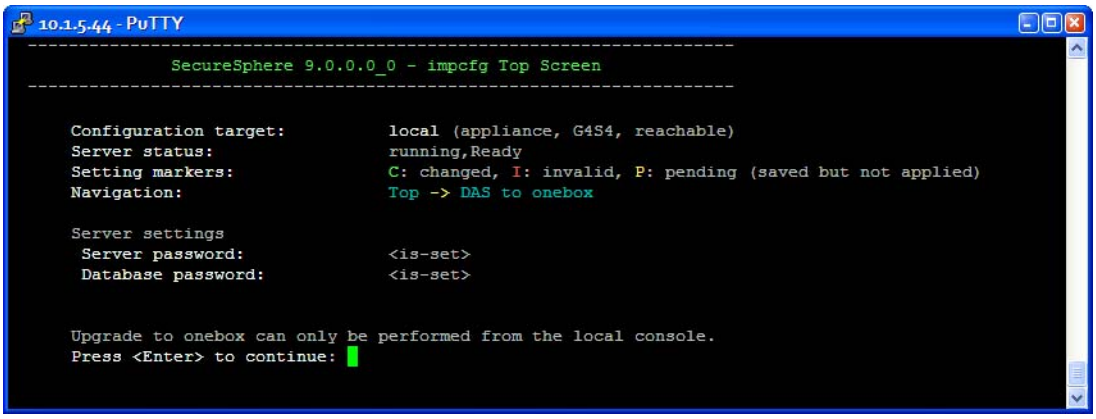


Figure 14 Reconfigure DAS as Onebox screen

Note: You will need to install a new license for the Onebox.

A message will be displayed stating that all IP configurations will be deleted and that you will have to rewire the network cables, and asking whether you want to continue.

2. Enter **`y`** to continue.

   `impcfg` will exit and you will be asked to run **`impcfg`** again.

3. Run **`impcfg`**.

   `impcfg` will start in it s initialization mode, that is, you will be asked to configure the appliance from scratch.

Configuring the Platform

You can:

- manage network and time settings, users and root password
- reboot/shutdown the appliance

To configure the platform:

1. In the **Top** Screen, select **3) Manage platform**. The **Platform Management** screen is displayed.

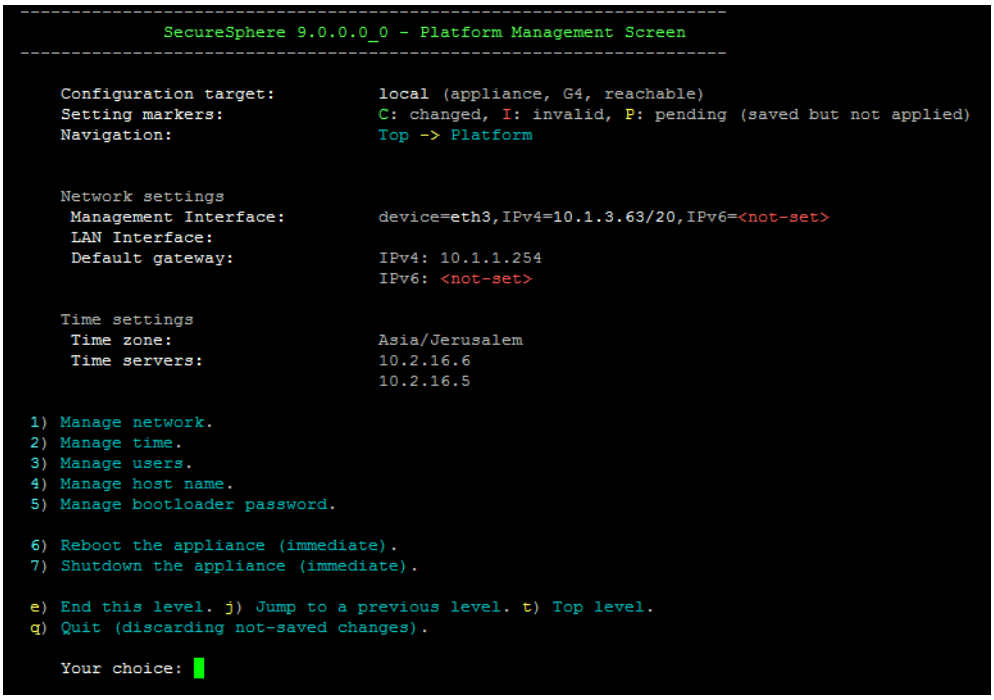


Figure 15 Platform Management screen

2. Select one of the following options, as listed below.

Platform Management Screen Configuration Options

Option	Name	Description
1	Manage network	Change the management and LAN interfaces, the default gateway, *etc*. For more information, see Network Management on page 85.
2	Manage time	Change the time zone, date and/or time, or configure NTP on the appliance. For more information, see Time Management on page 91.
3	Manage users	Manage CLI users. For more information, see Users Management on page 92.
4	Manage host name	Manage the appliance host name. For more information, see Hostname Management on page 97.

Platform Management Screen Configuration Options (continued)

Option	Name	Description
5	Manage bootloader password	Manage the bootloader (GRUB - Grand Unified Bootloader) password. For more information, see Bootloader Password Management on page 98.
6	Reboot the appliance (immediate)	Reboot the appliance.
7	Shutdown the appliance (immediate)	Shutdown the appliance.

Network Management

In the **Network Management** screen, you can:

- specify the management interfaces, and default gateway
- configure the DNS client
- locate network devices

To manage network settings:

1. In the **Platform Management** Screen (Figure 15 on page 84), select **1) Manage network**. The **Network Management** screen is displayed.

```
------------------------------------------------------------------------
             SecureSphere 9.0.0.0_0 - Network Management Screen
------------------------------------------------------------------------

   Configuration target:          local (appliance, G4, reachable)
   Setting markers:               C: changed, I: invalid, P: pending (saved but not applied)
   Navigation:                    Top -> Platform -> Network


C  Management Interface:          device=eth3,IPv4=10.1.3.63/20,IPv6=2001:db8::1:0:0:1/24
   LAN Interface:
   Default gateway:               IPv4: 10.1.1.254
                                  IPv6: <not-set>
   Static routes:                 <not-set>
   DNS Client:                    enabled=true,domain=il.imperva.com,search-list=<not-set>,servers=10.2.16.5

1) Management interface.
2) LAN interface.
3) IPv4 default gateway.
4) IPv6 default gateway.
5) Static routes.
6) Name resolution (DNS client).
7) Locate network devices.

e) End this level. j) Jump to a previous level. t) Top level.
q) Quit (discarding not-saved changes).

   Your choice:
```

Figure 16 Network Management screen

2. Select one of the following options, as listed below.

Network Management Screen Configuration Options

Name	Description
Management interface	Change the network interface and/or IP address (including CIDR) of the management interface. You can specify: • an IPv4 address only • and IPv6 address ony • both an IPv4 address and an IPv6 address Physically locate the network interface used as the management interface. For more information, see Management Interface on page 86.
LAN interface	Change the network interface and/or IP address (including CIDR) of the LAN interface. You can specify: • an IPv4 address only • and IPv6 address ony • both an IPv4 address and an IPv6 address Physically locate the network interface used as the LAN interface. For more information, see LAN Interface on page 88.
IPv4 default gateway IPv6 default gateway	Change the appliance's default gateway. Whether IPv4 or IPv6 default gateway options (or both) are available depends on whether the management interface and/or LAN interface has only an IPv4 or only an IPv6 address, or both. In the screen shown above, the management interface has both an IPv4 and and an IPv6 address, so both "IPv4 default gateway" and "IPv6 default gateway" options are listed in the menu. For more information, see Default Gateway on page 89.
Static routes	Add and delete static routes. For more information, see Static Routes on page 89.
Name Resolution (DNS client)	Enable or disable the DNS client. You must enable the DNS client if the management server will be using LDAP to authenticate SecureSphere administrators (see Authentication and Authorization Configuration on page 298). Define the domain name and search list, and specify a list of name servers. For more information, see Name Resolution (DNS client) on page 90.
Locate network devices	Physically locate an network interface. For more information, see Locate Network Devices on page 91.

Management Interface

In the **Management Interface** screen, you can:

- change the network interface and/or IP address (including CIDR)
- physically locate the network interface used as the management interface

To manage the management interface:

1. In the **Network Management** screen (Figure 16 on page 85), select **1) Management interface**. The **Management Interface** screen is displayed.

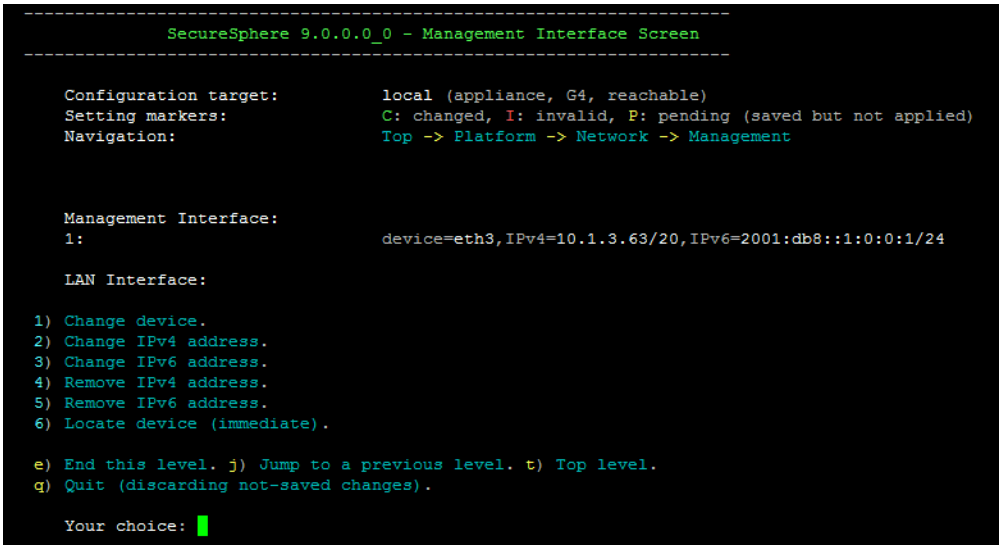


Figure 17 Management Interface Screen

2. Select one of the following options, as listed below.

Management Interface Screen Configuration Options

Name	Description
Set/Change device	Set or change the network interface to be used as the management interface. Specify the name, for example “eth4”, of one of the available network interfaces.
Set/Change IPv4 address Set/Change IPv6 address	Set or change the IP address of the network interface used as the management interface. Whether IPv4 or IPv6 address options (or both) are available depends on whether the management interface has only an IPv4 or only an IPv6 address, or both. In the screen shown above, the management interface has both an IPv4 and and an IPv6 address, so both “Change IPv4 address” and “Change IPv6 address” options are listed in the menu.
Remove IPv4 address Remove IPv6 address	Remove the IP address of the network interface used as the management interface. Whether IPv4 or IPv6 address options (or both) are available depends on whether the management interface has only an IPv4 or only an IPv6 address, or both. In the screen shown above, the management interface has both an IPv4 and and an IPv6 address, so both “Remove IPv4 address” and “Remove IPv6 address” options are listed in the menu.
Locate device (immediate)	This option will help you physically locate a network interface by attempting to blink one of the LEDs associated with the management network interface. **Note:** Before activating this option, disconnect, if possible, all the network cables attached to the device.

LAN Interface

In the **LAN Interface** screen, you can:

- change the network interface, IP address and netmask of the LAN interface
- physically locate the network interface used as the LAN interface

To manage the LAN interface:

1. In the **Network Management** screen (Figure 16 on page 85), select **2) LAN interlace**. The **LAN Interface** screen is displayed.

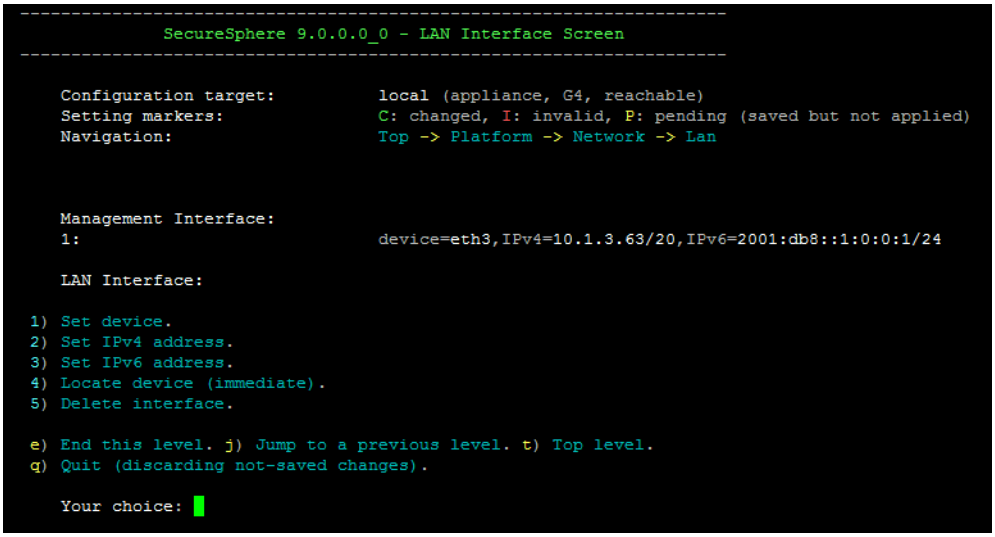


Figure 18 LAN Interface Screen

2. Select one of the following options, as listed below.

LAN Interface Screen Configuration Options

Name	Description
Set/Change device	Set or change the network interface to be used as the LAN interface. Specify the name, for example “eth4”, of one of the available network interfaces.
Set/Change IPv4 address Set/Change IPv6 address	Set or change the IP address of the network interface used as the LAN interface.
Locate device (immediate)	This option will help you physically locate a network interface by attempting to blink one of the LEDs associated with the LAN network interface. You will be asked to specify an Activation time. **Note:** Before activating this option, disconnect, if possible, all the network cables attached to the device.
Delete interface	

Default Gateway

You can:

- change the appliance's default gateway

To change the appliance's default gateway:

1. In the **Network Management** screen (Figure 16 on page 85), select **IPv4 Default gateway** or **IPv6 Default gateway**.
2. You will be asked to specify an IP address and, optionally, a device (network interface) for the default gateway.

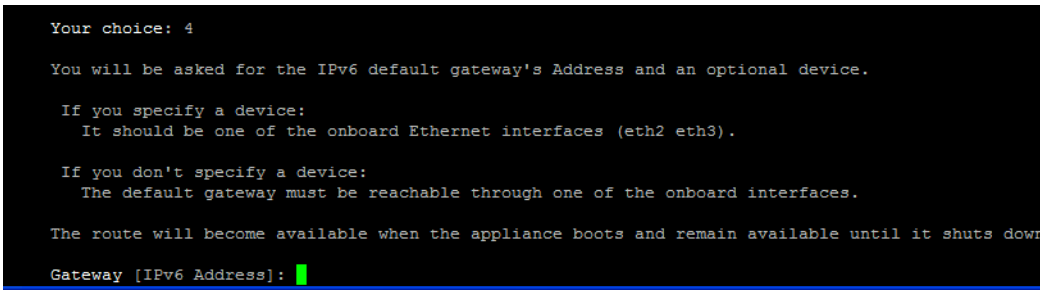


Figure 19 Default Gateway

Static Routes

In the **Static Routes** screen, you can:

- add and delete static routes

To configure static routes:

1. In the **Network Management** screen (Figure 16 on page 85), select **Static routes**. The Static Routes screen is displayed.

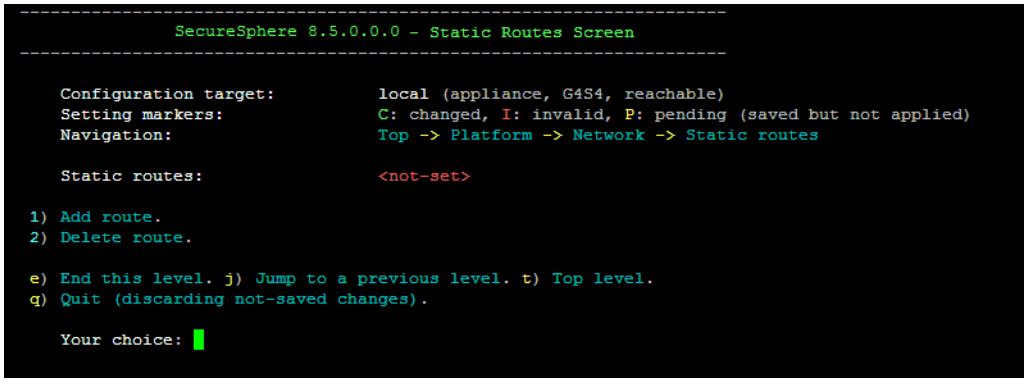


Figure 20 Static Routes Screen

2. Select one of the following options, as listed below.

Static Routes Screen Configuration Options

Option	Name	Description
1	Add route	Add a static route. You will be asked to specify the type (host or net), the IP address, the gateway and optionally, a network interface. When defining static routes, the user must define the device (interface). **`impcfg`** presents the user with a list of relevant devices (interfaces) as a hint, and the user should select one of these.

Static Routes Screen Configuration Options (continued)

Option	Name	Description
2	Delete route	Delete an existing static route.

Name Resolution (DNS client)

In the **DNS Client Configuration** screen, you can:

- enable or disable the DNS client
- define the domain name and search list
- specify a list of name servers

To configure DNS:

1. In the **Network Management** screen (Figure 16 on page 85), select **5) Name resolution (DNS client)**. The **DNS Client Configuration** screen is displayed.

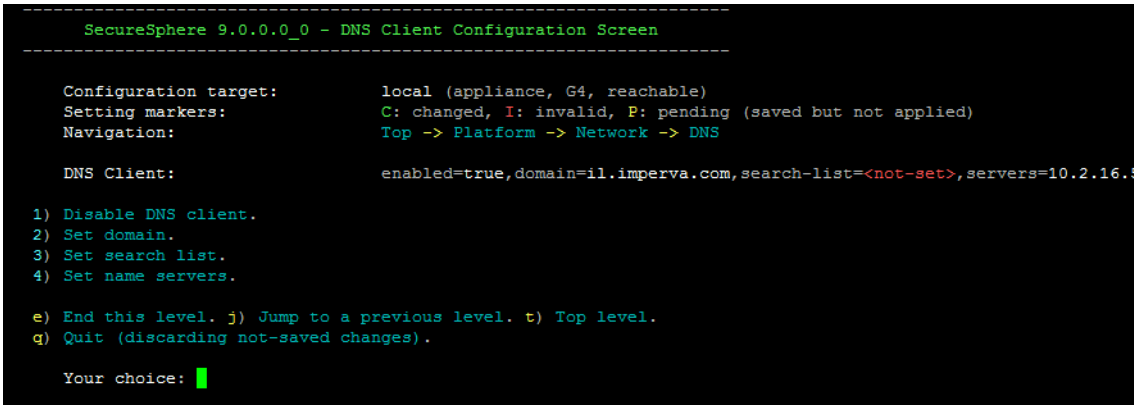


Figure 21 DNS Client Configuration

2. Select one of the following options, as listed below.

DNS Client Configuration Screen Configuration Options

Option	Name	Description
1	Enable/Disable DNS client	Enable or disable the DNS client. You must enable the DNS client if the management server will be using LDAP to authenticate SecureSphere administrators (see Authentication and Authorization Configuration on page 298).
2	Set domain	Define the domain name.
3	Set search list	Define the domain search list.
4	Set name servers	Specify a comma-separated list of name servers. Make sure these are real DNS servers, not “dummy” IP addresses.

Locate Network Devices

This option will help you physically locate a network interface by attempting to blink one of the LEDs associated with the network interface.

Note: Before activating this option, disconnect, if possible, all the network cables attached to the device.

To physically locate a network interface:

1. In the **Network Management** screen (Figure 16 on page 85), select **6) Locate network device**.
2. Select an interface from the list of available interfaces.
3. Specify an Activation time.

Time Management

You can:

- change the date, time, and time zone
- configure the NTP server.

To manage time settings:

1. In the **Platform Management** screen (Figure 15 on page 84), select **2) Manage time**. The **Time Management** screen is displayed.

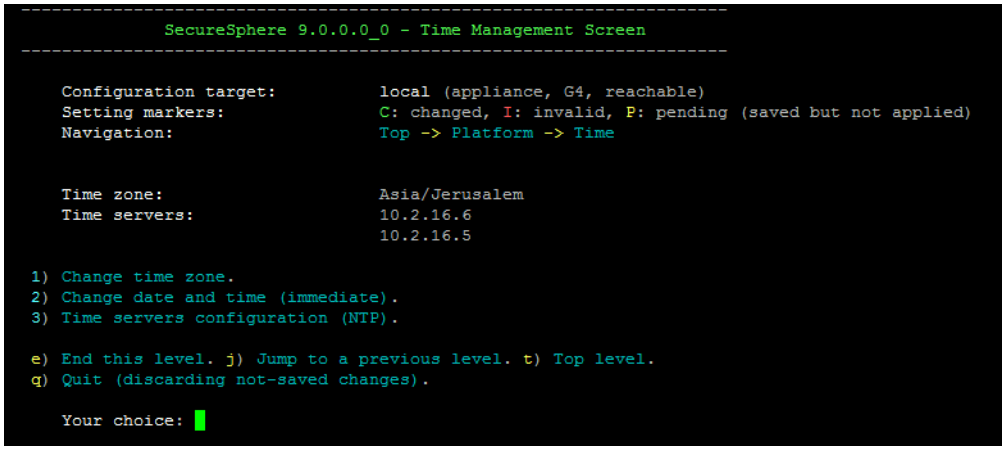


Figure 22 Time Management screen

2. Select one of the following options, as listed below.

Time Management Screen Configuration Options

Option	Name	Description
1	Change time zone	Change the appliance's time zone. You will be asked to select a time zone and then a country, or to specify the time zone using the Posix TZ format.
2	Change date and time (immediate)	
3	Time servers configuration (NTP)	For more information, see Time Servers on page 92.

Time Servers

You can:

- add and delete NTP servers

To manage NTP servers:

1. In the **Time Management** screen (Figure 22 on page 91), select **2) Manage time**. The **Time Management** screen is displayed.

   A list of previously-added time servers is displayed under **Time Server(s)**.

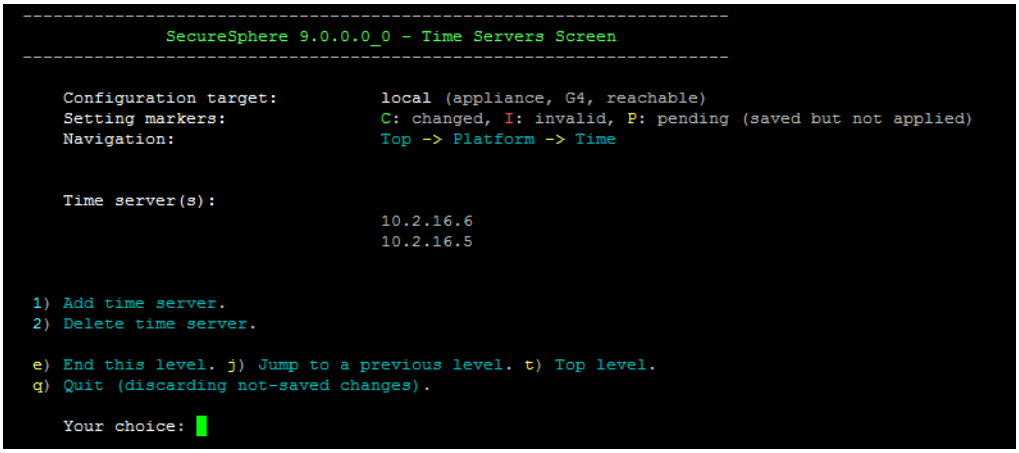


Figure 23 Time Servers screen

2. Select one of the following options, as listedlisted below.

Time Servers Screen Configuration Options

Option	Name	Description
1	Add time server	Add an NTP server. You will be asked to enter the IP address of the NTP server to be added. You can add an IPv4 address or an IPv6 address, depending on whether the appliance's LAN interface has an IPv4 or IPv6 address, or both. **Note:** Synchronization will be not take place if the time difference between the appliance and the NTP server is too great. You should manually set the time on the appliance to be correct (within 2-3 minutes) before the initial synchronization attempt.
2	Delete time server	Delete a previously-added NTP server. You will be asked to enter the IP address of the NTP server to be deleted. This must be one of the IP addresses displayed under **Time Server(s)**.

Users Management

You can:

- change the root user's password
- create a new user
- manage an existing user
- configure external authentication

To manage users:

1. In the **Platform Management** screen (Figure 15 on page 84), select **3) Manage users**. The **Users Management** screen is displayed.

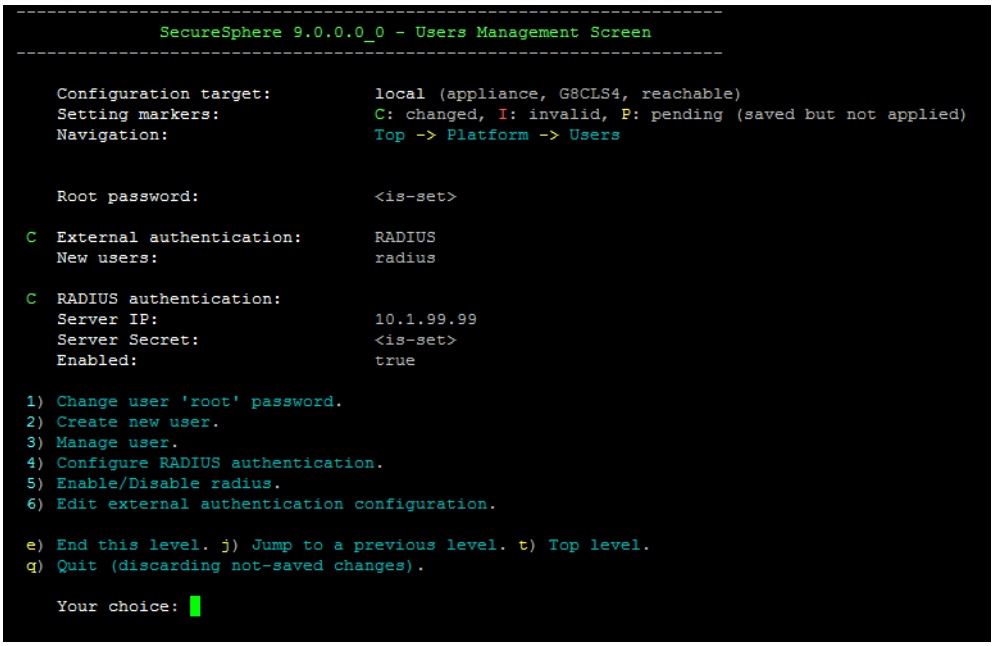


Figure 24 Users Management screen

2. Select one of the following options, as listed below.

Time Management Screen Configuration Options

Option	Name	Description
1	Change user ‘root’ password.	For more information, see Change Root User Password on page 93.
2	Create new user.	For more information, see Create New User on page 94.
3	Manage user.	For more information, see Manage User on page 95.
4	Configure RADIUS authetication.	For more information, see Configure RADIUS Authentication on page 96.
5	Enable / disable RADIUS.	For more information, see Configuring RADIUS Authentication on page 96.
6	Edit external authentication configuration.	For more information, see Edit External Authentication Configuration on page 97.

Change Root User Password

1. Enter the root user’s existing password.
2. Enter a new password for the root user.
   You can also enter the string “nochange”, in which case you will be returned to the previous menu.
3. Enter the new password again.

Create New User

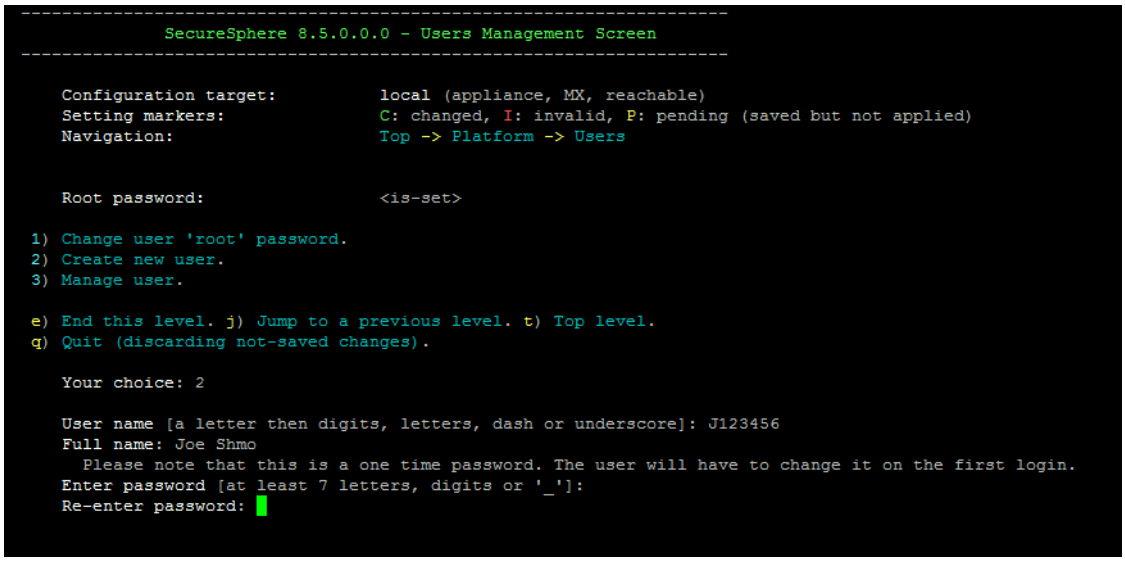


Figure 25 Creating a new user

1. Enter a User Name.

Note:
- The user name must begin with a letter followed by letters, digits, dash or underscore characters.
- You cannot create a user whose name is one of the existing system users, for example, root, secure, *etc*.
- User names are case-insensitive.

2. If the authentication method (see Configure RADIUS Authentication on page 96) is “user-defined” , you will be asked to specify whether authetication for this user is local or external.
   2.1 If you choose external, then you have finished creating the new user. All the information about the user will be obtained form the external authernitcation server (RADIUS) when the user logs in.
   2.2 If you choose “local”, then continue with the next step.
3. Enter a full name for the user (see example above in Figure 25).
4. Enter a password for the user.

   The password is a one-time password, and the user will have to change it when he or she logs in for the first time.
5. Enter the password again.

   The new user will be saved in the SecureSphere database when you apply the pending changes (**Apply changes** in the **Top** screen).

Manage User

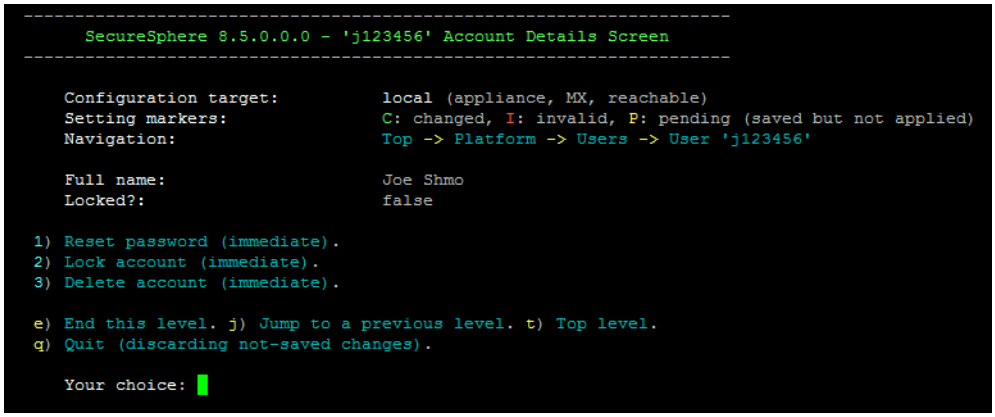


Figure 26 User Account Details screen

1. In the **User Account Details** screen (Figure 26), select one of the following options, as listed below.

User Account Details Options

Option	Name	Description
1	Reset password (immediate).	Reset (change) the user's password. You will be asked to enter a new password, and then to re-enter the same password. The password will be changed immediately. The new password is a one-time password, and the user will be asked to change it the next time he or she logs in. You can also enter the string "nochange", in which case you will be returned to the previous menu.
2	Lock account (immediate).	If the user's account is not locked, you can lock it by selecting this option.
2	Unlock account (immediate).	If the user's account is locked, you can unlock it by selecting this option.
3	Delete account (immediate).	Delete this user's account. You will be asked to confirm the deletion.

Configure RADIUS Authentication

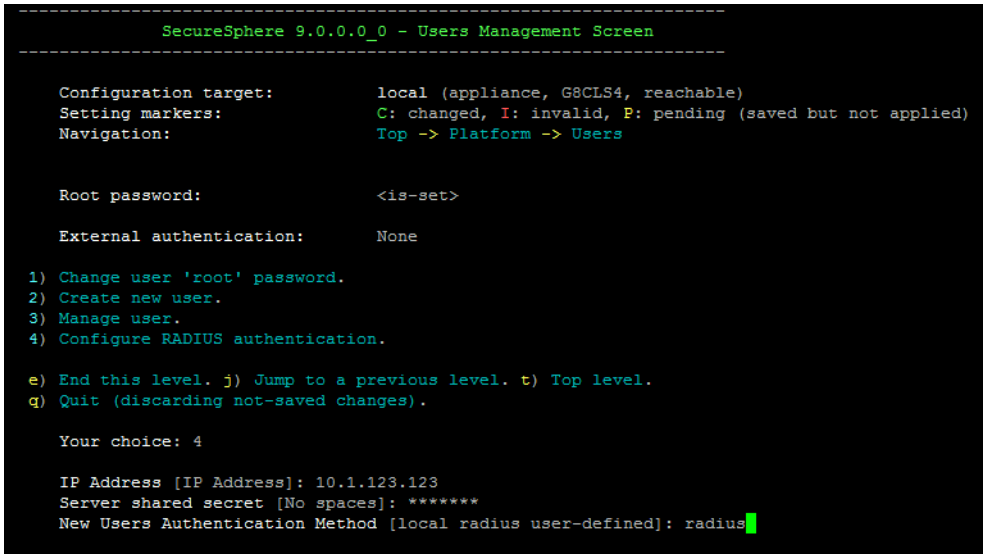


Figure 27 Configuring RADIUS Authentication

Specify the following information:

Name	Description
IP Address	The IP address of the RADIUS server.
Server shared secret	The shared secret between the RADIUS server and the SecureSphere appliance.
New Users Authentication Method	Select one of: • local - All new users will be authenticated by a passord, locally on the SecureSphere appliance. • radius - All new users will be authenticated by the RADIUS server. • user-defined - The authentication method for new users will be specified at the time they are created. For more information, see Create New User on page 94.



Note: To enable RADIUS authentication, you must also:
- Enable RADIUS (see Enable / Disable RADIUS and Edit External Authentication Configuration below).
- On the RADIUS server, establish trusted communication with the SecureSphere appliance.

Enable / Disable RADIUS

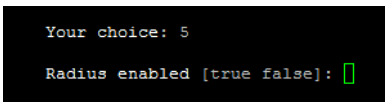


Figure 28 Enabling / Disabling RADIUS Authentication

Specify the following information:

Name	Description
RADIUS enabled	Specify “true” or “false”.

Note: CLI RADIUS authentication, supports only PAP. SecureSphere MX RADIUS authentication supports PAP, CHAP, and MS-CHAP.

Edit External Authentication Configuration

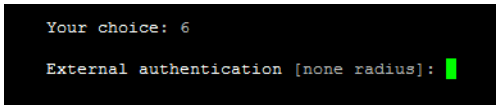


Figure 29 Enabling / Disabling external authentication configuration

Specify the following information:

Name	Description
External authentication	Specify “none” or “RADIUS”.

Hostname Management

You can:

- change the hostname.

To manage the hostname:

1. In the **Platform Management** screen (Figure 15 on page 84), select **4) Manage host name**. The **Hostname Configuration** (Figure 30 on page 97) screen is displayed.

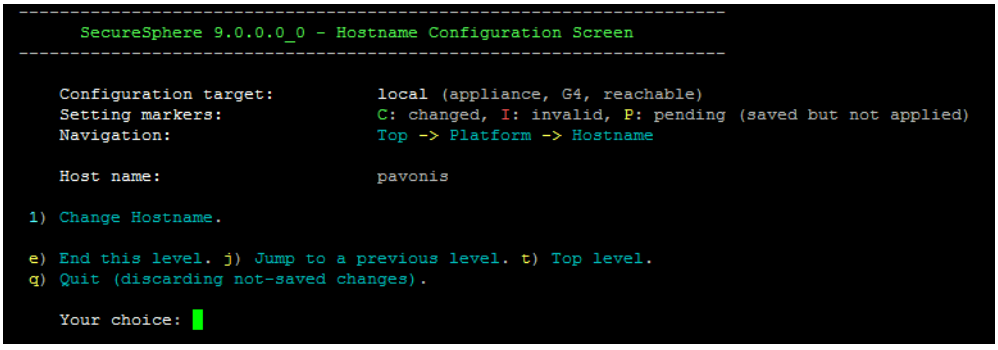


Figure 30 Hostname Configuration screen

2. Select one of the following options, as listed below.

Time Management Screen Configuration Options

Option	Name	Description
1	Change Hostname	Change the appliance’s hostname.

Bootloader Password Management

1. Enter the bootloader user's existing password.
2. Enter a new password for the bootloader user.
   You can also enter the string "nochange", in which case you will be returned to the previous menu.
3. Enter the new password again.

Configuring SecureSphere Routes

You must define the SecureSphere routes listed in Table using `impcfg`.

Static Routes Screen Configuration Options

Routes	Description	Data stored in
Platform routes	These routes are related to the appliance, management server or gateway, management interfaces. For more information, see Static Routes on page 89.	• `/etc/sysconfig/static-routes` (executed at boot time) • `bootstrap.xml`
Kernel Reverse Proxy Apache Reverse Proxy Remote Agent	These routes are executed and added automatically according to the gateway mode. They are deleted when the gateway is stopped with the "`teardown`" option, and added when the gateway is started with the "`prepare`" option. For more information, see: • Configuring Kernel Reverse Proxy on page 103 • Configuring Apache Reverse Proxy on page 110 • Configuring Remote Agent Routes on page 99	`bootstrap.xml`
VRRP listeners for agents VRRP Reverse Proxy	These routes are executed with relation to the VRRP status, either master or backup. For more information, see Configuring VRRP Routes on page 100.	`/etc/keepalived.conf`

Configuring Remote Agent Routes

To configure Remote Agent routes:

1. In the **Top** Screen, select option **1) Manage gateway.** The **Gateway Management** screen is displayed.
2. In the **Gateway Management** screen, select **6) Manage Remote Agents.** The **Remote Agents** screen is displayed

3. In the **Remote Agents** screen, select **6 - Manage remote-agent related routes**. The **Remote Agent Routes** screen is displayed.

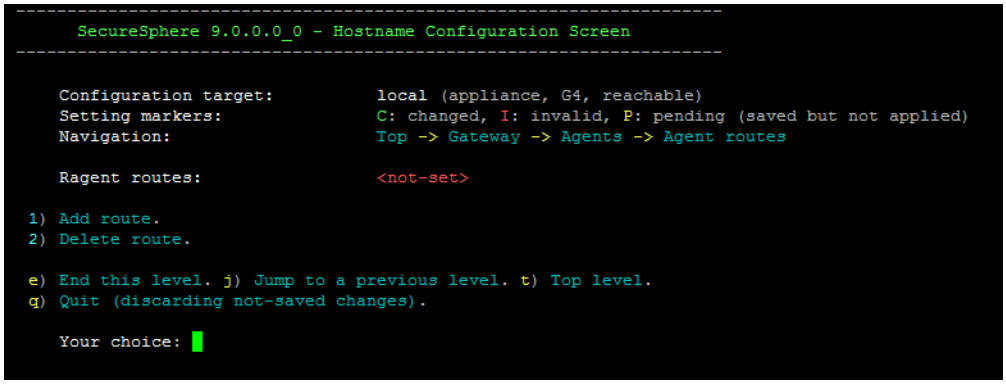


Figure 31 Remote Agent Routes screen

4. Select one of the following options, as listed below.

Reverse Proxy (apache) Screen Configuration Options

Option	Name	Description
1	Add Route	Add a route.
2	Delete Route	Delete a route.

Configuring VRRP Routes

Note: With VRRP, both gateways must be in the same subnet.

To configure VRRP routes:

1. In the **Top** Screen, select option **2) SecureSphere Gateway**. The **Gateway Management** screen is displayed.
2. In the **Gateway Management** screen, select **7) Manage interfaces and routes**. The **Reverse Proxy (kernel)** screen is displayed.

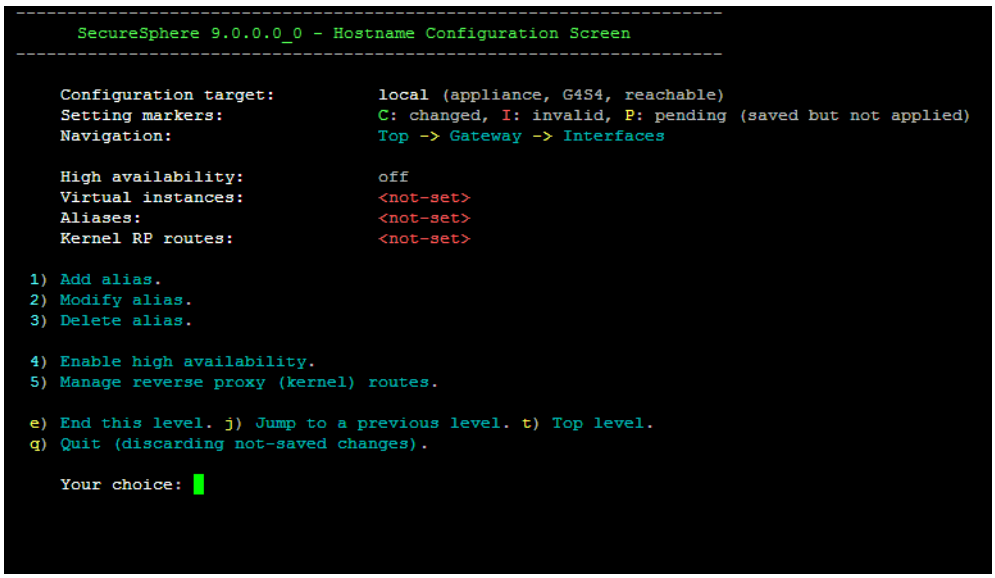


Figure 32 Reverse Proxy (kernel) screen

3. Select **5) Manage reverse proxy (kernel) routes**. The **Reverse Proxy Kernel Routes** screen is displayed.

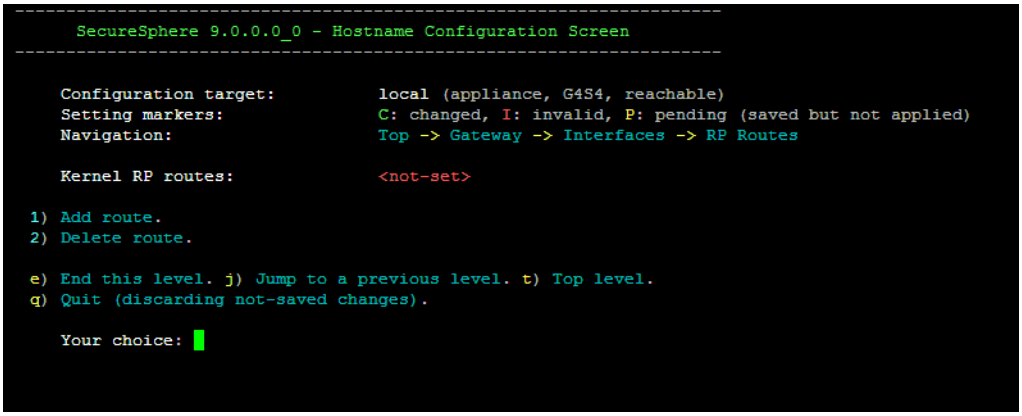


Figure 33 Reverse Proxy Kernel Routes screen

4. Select one of the following options, as listed below.

Static Routes Screen Configuration Options

Option	Name	Description
1	Add route	Add a route.
2	Delete route	Delete a route.

Configuring Transparent Reverse Proxy

To configure Transparent Reverse Proxy, perform the following tasks after the First Time Login is complete, as listed below.

Transparent Reverse Proxy Configuration Task Overview

	Task Overview	Step-By-Step
1	In `impcfg`, configure the appliance as a bridge.	**Manage SecureSphere Gateway** > **Change operation mode** and select **Bridge STP** or **Bridge IMPVHA**.
2	In the SecureSphere GUI, configure the server group. For more information, see ***SecureSphere User Guide***.	In the **Transparent Reverse Proxy** section of the **Definitions** tab of the server group (**Main** > **Setup** > **Sites**), select **Enable Transparent Reverse Proxy**.
3		Define the server IP addresses and ports for which the gateway will act as Transparent Reverse Proxy.



Note: In the event of a conflict between a Transparent Reverse Proxy rule (**Main** > **Setup** > **Sites**) and another service's port configuration, the Transparent Reverse Proxy rule takes precedence.

Configuring Kernel Reverse Proxy

This section contains the following:

- Before Configuring the Kernel Reverse Proxy on page 103
- Configuring Routing on page 107



Note: For information about configuring Kernel Reverse Proxy and Apache Reverse Proxy on the same gateway, see Configuring Kernel Reverse Proxy and Apache Reverse Proxy on the Same Gateway on page 117.

Before Configuring the Kernel Reverse Proxy

Before configuring the gateway and management server:

1. Prepare a list of the IP addresses for the KRP inbound and outbound interfaces.

   If you are deploying KRP and ARP on the same SecureSphere gateway, the KRP's outbound interface will be the loopback interface.
2. If the gateway and the backend server are not in the same network, configure the routing accordingly.
3. Prepare the redirection rules (based on hostnames and/or URLs) for the KRP decision rules.
4. If you plan to implement VRRP for High Availability, prepare the IP addresses accordingly.

Configuring the Kernel Reverse Proxy

This section contains the following:

- Changing the Gateway's Mode to KRP on page 103
- Configuring Aliases on page 105
- Configuring Routing on page 107

Changing the Gateway's Mode to KRP

If, during the First Time Login, you configured the gateway as KRP, then you can skip this step.

Otherwise, follow these instructions.

To configure a gateway as a Kernel Reverse Proxy:

1. In the **Gateway Management** screen (Figure 3 on page 71), select option **4) Change operation mode**.
2. From the list of operation modes (Figure 5), select **6) Reverse Proxy Kernel**.

3. In the **Gateway Management** screen (Figure 3 on page 71), select option **7) Manage interfaces and routes**. The **Reverse Proxy Kernel** screen is displayed.

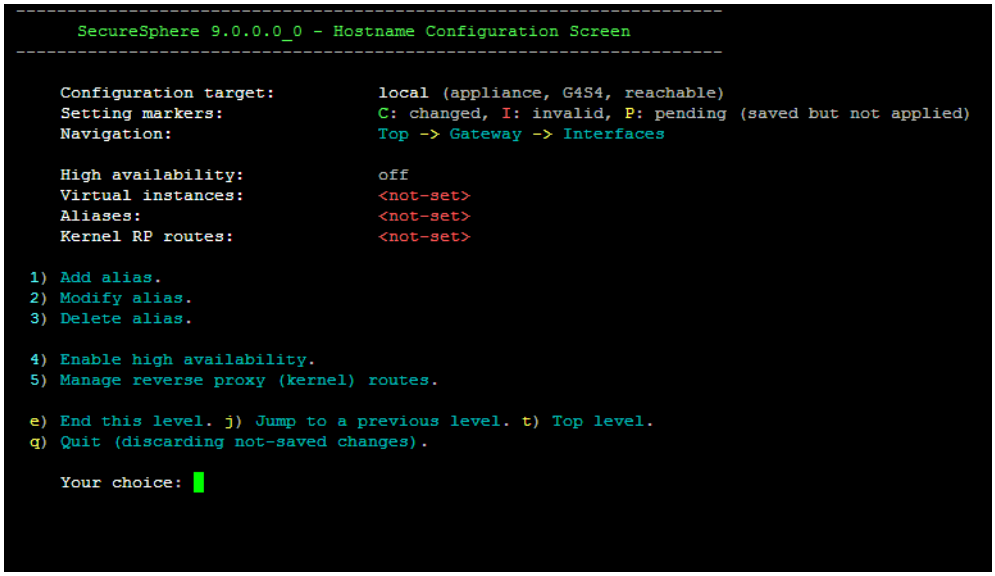


Figure 34 Reverse Proxy (kernel) screen

4. Select one of the following options, as listed below.

Reverse Proxy Kernel Screen Configuration Options

Option	Name	Description
1	Add alias	An alias consists of an alias name and a pair of the following (see Figure 35): • device (for example, eth2) • IP address • netmask These aliases will appear in the SecureSphere GUI (in the **Reverse Proxy** section of the **Definitions** tab of the server group (**Main** > **Setup** > **Sites**). For more information, see Adding an Alias on page 105.
2	Modify Alias	For more information, see Modifying an Alias on page 106.
3	Delete Alias	For more information, see Deleting an Alias on page 106.
4	Enable high availability	For more information, see Chapter 16, Gateway High Availability.
5	Manage reverse proxy (kernel) routes	For more information, see Configuring SecureSphere Routes on page 99.

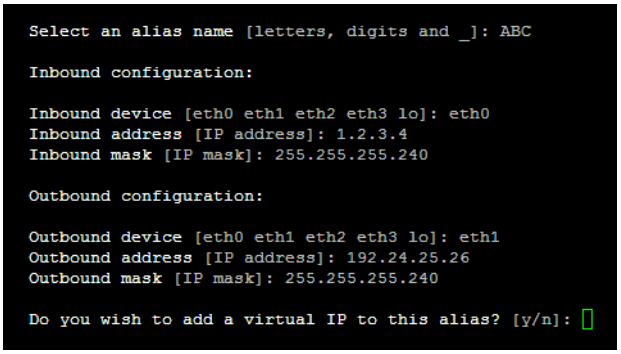


Figure 35 Defining an Alias

Configuring Aliases

An alias represents the inbound IP address and the outbound IP address for the KRP. Since a network tends to be dynamic, IP address allocation may change from time to time. Aliases eliminate the need to configure changes in two places (on the gateway and on the management server). For multiple end points (servers), you can use port mapping (one gateway IP address with multiple ports). Alternatively, use an alias representing a reverse proxy IP address per server so that whenever an alias is addressed, the communication will be forwarded to the corresponding server.

To configure an alias:

1. In the `impcfg` **Top** screen (Figure 1 on page 61), select **2) Manage SecureSphere Gateway**.
2. In the **Gateway Management Screen** (Figure 3 on page 71), select **7) Manage interfaces and routes**.
3. Select one of the following options, as listed below.

Manage Interfaces and Routes Screen Configuration Options

Option	Name	Description
1	Add alias	For more information, see Adding an Alias on page 105.
2	Delete Alias	For more information, see Deleting an Alias on page 106.
3	Modify Alias	For more information, see Modifying an Alias on page 106.

Adding an Alias

4. To add an alias, enter the alias' parameters, as listed below.

Alias Parameters

Parameter	Description
Select Alias Name	The alias names appear in the GUI, so select logical names that help users to identify the servers. Use alphanumeric characters.
Inbound device	The physical interface that receives traffic from clients. Choose one of the appliance interfaces of the device (not the management interface): eth1, eth2, eth3, eth4, eth5.
Inbound address	The IP address to which clients connect.
Inbound mask	The inbound IP address mask.

Alias Parameters (continued)

Parameter	Description
Outbound device	The physical interface that forwards the traffic to the web server. Choose one of the appliance interfaces of the device (not the management interface): eth1, eth2, eth3, eth4, eth5. **Note:** If you are deploying KRP and ARP on the same appliance, then the KRP should output to the loopback interface. When the one arm topology is used, you can choose the same device as the inbound device.
Outbound address	The IP address which is used by the KRP to communicate with the web server. When the one arm topology is used, you can choose the same IP address as the inbound IP address, though it is recommended to choose a different IP address.
Outbound mask	The outbound IP address mask.
Do you wish to add a virtual IP to this alias?	Choose **n**, unless you are using VRRP and High Availability Gateways. For more information, see Configuring the Gateway for High Availability on page 108. Possible values: `y` | `n`

5. Repeat the previous two steps for each alias you wish to create.
6. When you have completed configuring all your aliases, enter **t** to navigate to the **Top** screen.
7. In the **Top** screen, apply the changes by selecting **A) Apply settings**.
8. Save the changes by selecting **S) Save settings**.
9. Confirm that the aliases were correctly configured by executing the following command:

```
ip -4 a
```

   This command lists the IP addresses and the interfaces on which the gateways listens.
10. If the alias IP addresses you have just configured are not listed, then restart the gateway by executing the following commands:

```
impctl gateway stop --teardown
impctl gateway start --prepare
```

11. For each alias you add, you must add a decision rule is a redirection rule with priority, and defines what traffic KRP handles and how it is redirected to the backend server.

    For information on how to configure a KRP, including decision rules, see the “Configuring a Kernel (Non-Transparent) Reverse Proxy” section in the Reverse Proxies chapter of the ***SecureSphere User Guide***.

Deleting an Alias

To delete an alias, enter the name of the alias.

Modifying an Alias

To modify an alias, enter the name of the alias and then change its parameters when prompted (see Table).

Configuring Routing

If the KRP's IP addresses (usually outbound addresses) are not on the same network as the destination IP addresses, routing must be configured to enable connectivity. If the default route was changed, it is important to configure new routes (for example, SSH to the gateway).

Note: If the backend server is not on the same network as the SecureSphere gateway, make sure communication is allowed through firewalls.

Reverse proxy routes are maintained in the `bootstrap.xml` file and executed and added automatically when the gateway starts. They are deleted automatically when the gateway is torn down (`impctl gateway stop --teardown`). For more information about SecureSphere routes, see Configuring SecureSphere Routes on page 99.

A typical routing configuration is shown in Figure 36.

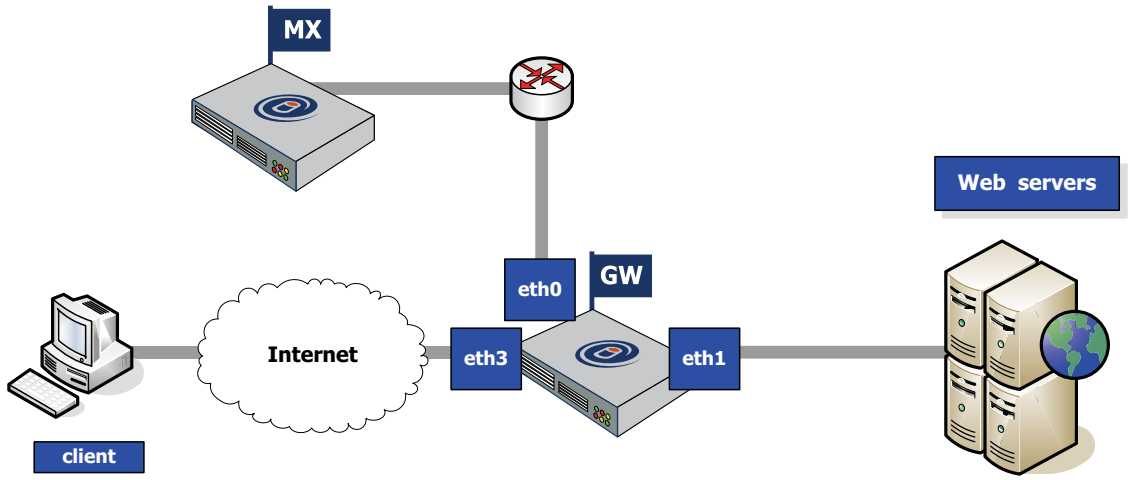


Figure 36 Typical Reverse Proxy Routing

There are two static routes to be configured:

- **eth0**: to the SecureSphere Management Server (MX)
- **eth1**: to the Web server

All other traffic can be routed out through the Internet. The challenge here is to ensure that the Management Server traffic is properly routed out through eth0.

To define a KRP route:

1. In the `impcfg` **Top** screen (Figure 1 on page 61), select option **2) Manage SecureSphere Gateway**.
2. In the **Gateway Management Screen** (Figure 3 on page 71), select **7) Manage interfaces and routes**.
3. In the **Reverse proxy (kernel) Screen** (Figure 32 on page 100), select **5) Manage reverse proxy (kernel) routes**.
4. To add a route, select **Add route** and enter the parameters, as listed below.

Route Parameters

Parameter	Description
Type	Defines whether this route is per subnet or specific to host. Possible values: `net` | `host` Enter `host`, unless you want the route to be valid for the whole network.
Address	Available only when the type host is selected. Enter the IP address of the destination host.

Route Parameters (continued)

Parameter	Description
Network	Available only when the **Type** is `net`. The IP address of the network is based on the network subnet. For example, if the server host IP is 10.3.220.22 and its subnet mask is 255.255.255.0, the net IP is 10.3.220.0 and the host IP is 10.3.220.22.
Subnet mask	Available only when the **Type** is `net`. The subnet mask of the network. Based on the example above, the net subnet mask is 255.255.255.0
Gateway	Specify the default gateway IP address, which is used for the listener. The default gateway IP address must be from inbound or outbound aliases networks.
Device	Specify the specific gateway physical interface to use or Enter for none. If none is selected, the best available interface is selected when routing.

5. To delete a route, select **Delete route** and choose the route to delete from the list of available routes.

Configuring a Server Group and Service

For information on how to configure a server group and service, see the ***SecureSphere User Guide***.

Configuring KRP and Decision Rules

A decision rule is a redirection rule with priority, and defines what traffic KRP handles and how it is redirected to the backend server.

For information on how to configure a KRP, including decision rules, see the "Configuring a Kernel (Non-Transparent) Reverse Proxy" section in the Reverse Proxies chapter of the ***SecureSphere User Guide***.

Configuring High Availability for KRP

High Availability for this configuration is available using VRRP (Virtual Router Redundancy Protocol).

To configure High Availability, you must configure the gateway and the management server.

Configuring the Gateway for High Availability

You must configure each of the gateways participating in the VRRP High Availability deployment.

Set the Gateway's Mode to KRP

To change the gateway's mode to KRP, follow the instructions in Configuring the Kernel Reverse Proxy on page 103.

Enable High Availability

To enable High Availability:

1. In the `impcfg` **Top** screen (Figure 1 on page 61), select **2) Manage SecureSphere Gateway**.
2. In the **Gateway Management Screen** (Figure 3 on page 71), select **7) Manage interfaces and routes**.
3. In the **Reverse proxy (kernel)** screen, select **4) Enable high availability**.

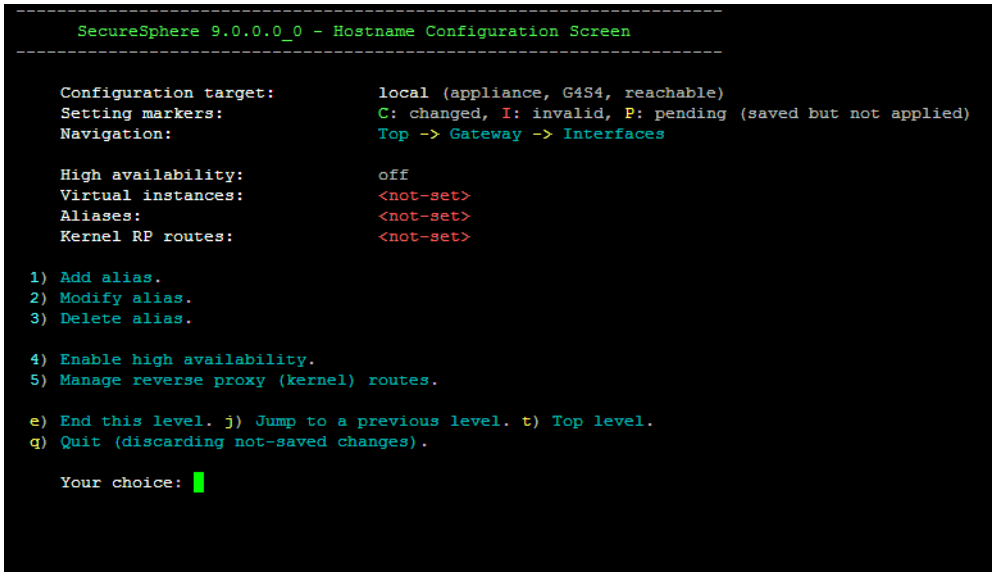


Figure 37 Reverse proxy (kernel) screen

Configure Aliases

To configure aliases, follow the instructions in Configuring Aliases on page 105.

- For each alias, set **Do you wish to add a virtual IP to this alias?** to **y**.

Configure Virtual Instances

1. In the `impcfg` **Top** screen (Figure 1 on page 61), select **2) Manage SecureSphere Gateway**.
2. In the **Gateway Management Screen** (Figure 3 on page 71), select **7) Manage interfaces and routes**.
3. Configure the virtual instance (the virtual IP address to be used by VRRP).

Configuring the Management Server for High Availability

For information on configuring High Availability for management servers, see Chapter 17, Management Server High Availability (MX-HA).

Configuring Apache Reverse Proxy

This section contains the following:

- Changing the Gateway's Mode to ARP on page 110
- Configuring ARP on page 110
- RSA Clear Trust Single Sign On (SSO) on page 112



Note:
- For information about using RSA Clear Trust Access Manager Single Sign On with Apache Reverse Proxy, see RSA Clear Trust Single Sign On (SSO) on page 112.
- For information about configuring Kernel Reverse Proxy and Apache Reverse Proxy on the same gateway, see Configuring Kernel Reverse Proxy and Apache Reverse Proxy on the Same Gateway on page 117.

Changing the Gateway's Mode to ARP



Warning: Skip this step if either of the following is true:
- During the First Time Login, you configured this gateway as ARP.
- This gateway will be configured with both KRP and ARP, in which case it must be configured in `impcfg` as KRP.

Otherwise, follow these instructions.

To configure a gateway as an Apache Reverse Proxy:

1. In the **Gateway Management** screen (Figure 3 on page 71), select option **4) Change operation mode**.
2. From the list of operation modes (Figure 5), select **4) Reverse Proxy Apache**.

Configuring ARP

Configuring Apache Reverse Proxy consists of the following:

- changing the HTTP listener port
- configuring the `httpd.conf` file to include the protected hosts (virtual hosts)

To configure Apache Reverse Proxy:

1. Log on to the gateway as the user `root`.
2. `cd` to the directory where the default Apache configuration file is located (`/etc/httpd/conf/httpd.conf`).
3. Back up the following files:
   - `httpd.conf`
4. Edit `httpd.conf` using a text editor (for example, `vi`).
5. Look for the following string: `Listen 80`
6. Comment out the line containing the above string by inserting the `#` character at the beginning of the line.
7. Add a new listening port.

   If ARP will be deployed together with KRP on this gateway, then the listening port should be restricted to the loopback interface.

   In any case, the listening port should be restricted to the protected host.

8. The protected host is defined inside the virtual host tags. Each protected host has its own virtual host definition. Change the backend server IP address according to your setup.

   If you decide to use fully qualified domain names, you must have a resolving mechanism in place. To achieve this, configure the DNS server using **impcfg** or both.

9. Add the following at the end of the **httpd.conf** file:

```
Listen 127.0.0.1:88
NameVirtualHost X.X.X.X:88
<VirtualHost X.X.X.X:88>
       ServerName 10.3.220.22
       DocumentRoot /var/www/html/
       ProxyPreserveHost On
       RewriteEngine On
       RewriteRule ^/(.*) http://Y.Y.Y.Y/$1 [P]
       Header unset "WWW-Authenticate: NTLM"
       Header add WWW-Authenticate "Basic realm=SERVER-NAME"
</VirtualHost>
```

   If ARP and KRP are deployed on the same SecureSphere gateway, then X.X.X.X should be **127.0.0.1** (the loopback interface)**.**

   Y.Y.Y.Y is the backend server on port 80 (default to HTTP).

   For example, to redirect to the backend server 10.3.220.22 on port 90, the **RewriteRule** line would be:

   RewriteRule ^/(.*) http://10.3.220.22:90/$1 [P]

10. Repeat the last step for any additional hosts you may need to use. If you need to redirect to multiple servers, use different ports, where each port represents a server. The ports should not be already in use by another process.
11. Save the file.
12. Close the file.

    httpd.conf includes the **nss.conf** file, which is configured to listen to port 443. To avoid conflicts when ARP and KRP are deployed on the same SecureSphere gateway, and KRP is configured to listen to port 443, comment out or reconfigure Apache to listen on a different port, as follows:

    cd to the **/etc/httpd/conf.d** directory.

13. Edit **nss.conf** using a text editor (for example, **vi**).
14. Look for the following string: **Listen 443**
15. Comment out the line containing the above string by inserting the **#** character at the beginning of the line.
16. Save the file.
17. Close the file.
18. Restart the HTTPD service by executing the following command:

    service httpd start

The following is displayed on the screen:

starting httpd: [OK]

If the status is something other than **[OK],** there is probably a conflict preventing the service from starting. Consult the Apache error log for details at **/etc/httpd/logs/error_log**.

For example, port conflict can prevent the service from starting.

19. Force **httpd** to start after reboot. by executing the following command:

    ln -s /etc/init.d/httpd /etc/rc3.d/S99zhttpd

20. **Optional**: To check which ports are included in your configuration, execute the following command:

    ```
    netstat -na | grep -I listen
    ```

    This command lists all ports, not only the ones you have configured. On a Onebox appliance, it lists the server ports as well.



Note: The `/etc/httpd/logs/error_log` file logs debug information for the Apache configuration. Apache log levels are set up by default at `httpd.conf`. The `LogLevel` tag controls the number of messages logged to the error_log. Possible values include: `debug`, `info`, `notice`, `warn`, `error`, `crit`, `alert`, `emerg`.

Encryption (SSL)

Apache encryption to the backend server is not supported.



Note: If you are redirecting from HTTP to HTTPS or vice versa, make sure server hyper links are relative

RSA Clear Trust Single Sign On (SSO)

RSA Clear Trust Overview

SecureSphere supports RSA Clear Trust Access Manager Single Sign On when using Apache Reverse Proxy. The prerequisites are:

- Clear Trust Access Manager (version 6.0)
- Access Manager Agent (version 4.7)
- Access Manager Server
- Dispatcher Server (installed on the same machine as the Access Manager Server)
- Imperva SecureSphere (version 6.2.0.6442 and higher)

It is assumed that:

- Clear Trust is configured with appropriate user rights on the relevant applications served by the Apache Reverse Proxy.
- All traffic requiring Single Sign On passes through the Apache Reverse Proxy.



Note: If Access Manager Server is not running on the SecureSphere gateway, you must ensure that communication between the two is allowed to pass through firewalls.

The Access Manager Agent should be installed on the SecureSphere gateway, and intercepts connections to the backend server. If the Clear Trust Access Manager rules specify that a connection should be authenticated, the following sequence of events occurs:

1. Access Manager Agent takes control of the connection and displays an RSA Access Manager Login web form.
2. The end user is redirected to the authentication page.
3. If the user successfully logs in, he is directed to the relevant content page.

   Session cookies are used to identify the user.
4. The user provides credentials to the RSA Access Manager Agent.
5. The RSA Access Manager Agent sends the credentials to the RSA Access Manager Server.
6. The RSA Access Manager Server verifies the credentials and whether the user is authorized to access the requested URL.
7. The RSA Access Manager Server sends the client an SSO cookie that enables future logins.

8. SecureSphere associates the login information with the web session, and any alerts generated during the session are also associated with the user.



Note: Since authentication to the Access Manager is form based, SecureSphere's user tracking engine learns the authentication process and identifies successful logins. If this web user has a security violation and an alert is issued, the alert will contain the Access Manager username. Changes to the AUT decision rules may needed.

Installing the RSA Access Manager Agent on the SecureSphere Gateway

1. On the SecureSphere gateway, install RSA Access Manager Agent version 4.7.

   This is the version that was tested and complies with both SecureSphere 6.2.0.6442 and Apache version 2.2.3
2. Change to the directory where the agent is installed
3. Run the interactive configuration script to configure the agent for the first time:

   `configure-apache2.sh`
4. Follow the instructions as displayed in Figure 38 on page 114.

   Here are some guidelines:
   - Apache server installation path on the SecureSphere gateway is **`/usr/bin`**
   - The path to **`httpd.conf`** is **`/etc/httpd/conf/httpd.conf`**
   - The path to the Apache binary is **`/usr/sbin/httpd`**
   - Web server host name: host name (or IP address) served by the Apache server.

     In other words, this is the client requested destination server name as it appears in the hostname header.
   - Web server domain name for cookie set up: Use the domain name served by Apache; alternatively use the host IP address.
   - Connection mode: Applies to the connection between the agent and the Access Manager Server. In this example we use: **clear**.
   - Dispatcher server IP and port: The address of the dispatcher key server in the format of **`hostname:port`**. In this example, it on the same machine as the Access Manager server **`10.1.13.159`** and the port number is **`5608`**.
   - Authorization server list: Enter list of authorization server or **`n`** if none is used.
   - Enter inter-site sign on: default **`n`**.



Note: You can edit the configuration file **`webagennt.conf`** in the Access Manager Agent home directory.

```
Configuring RSA Access Manager Agent 4.7 for Apache2
Apache web server installation path []: /usr/bin/
Unable to locate the apache config file. Enter path? (y/n) [n]: y
Path to httpd.conf: /etc/httpd/conf/httpd.conf
Unable to locate the apache binary (httpd). Enter path? (y/n) [n]: y
Path to httpd: /usr/sbin/httpd

Apache 2.2.3 detected.


Directory name [apache_2.2.3]:

Backing up original /etc/httpd/conf/httpd.conf
  to /etc/httpd/conf/httpd.conf.ctbak.

Configuring webagent.conf parameters:
Setting log file parameter.

Enter Web server host name [Soy]: 10.3.100.100

Webserver domain name for cookie setup [(none)]: 10.3.100.100
 [1] Clear
 [2] Anonymous
 [3] Authenticated
Choose Connection mode [2]: 1

Enter a comma-separated list of Dispatcher servers(hostname:port).
Dispatcher Server List [Soy:5608]: 10.1.13.159:5608

Enter Authorization Server List? (y/n) [n]:

Enable Inter-Site Sign-On(ISSO)? (y/n) [n]:

+-------------------------------------------------------------------------------+

  RSA Access Manager Agent 4.7 for Apache2

  Configuration complete.

  You can modify Agent settings by editing this configuration
  file as needed:

      /tmp/sso/agent-47-apache2/webservers/apache_2.2.3/conf/webagent.conf

  Use the RSA Access Manager Administrative Console to define policies for
  protecting specific resources on the server.

+-------------------------------------------------------------------------------+
```

Figure 38 RSA Access Manager Agent Installation

At this stage the Access Manager is part of the Apache Server. This happens by including the Access Manager Agent configuration file **`ct-httpd.conf`** in the Apache **`httpd.conf`** file. Each request from Apache to the backend server will be intercepted by the Access Manager Agent. A user who is required to login is redirected by the agent to the login page on the original hostname, for example, **`http://hostname/cleartust/ct_logon_en.html`**.

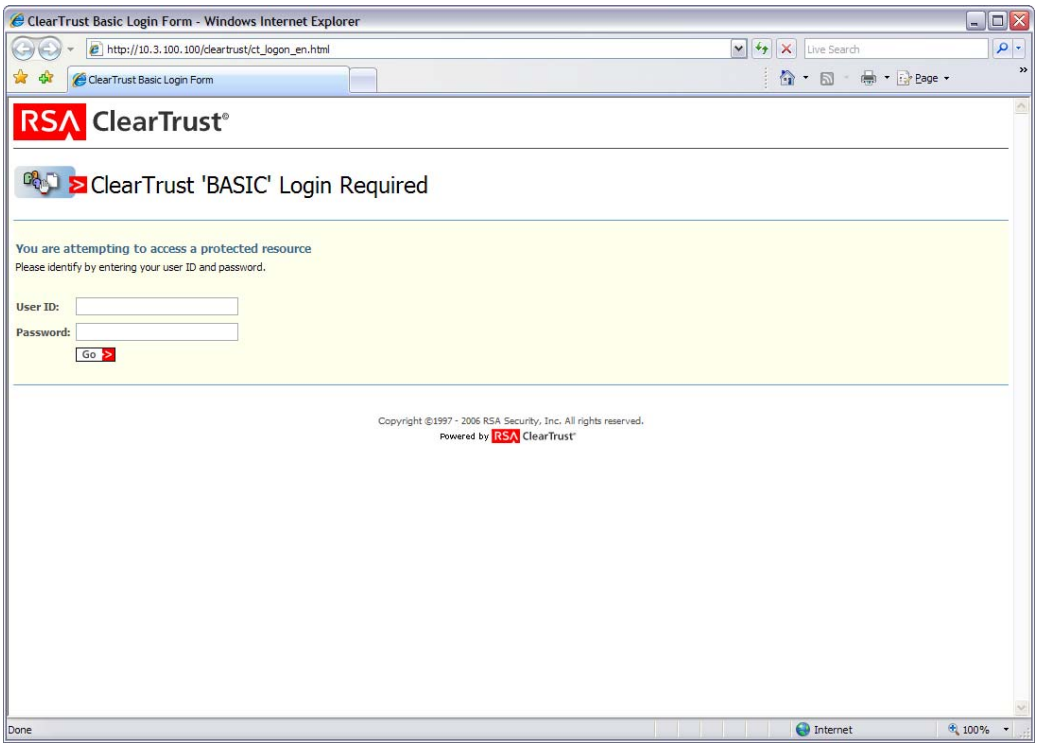


Figure 39 ClearTrust Login Page

5. To avoid intercepting the actual redirection to the login page (which includes the word `cleartrust` in its path) Apache must be reconfigured.

   For every virtual host (defined in `httpd.conf`) served by Apache and the Access Manager Agent, edit the Apache rewrite rule to include the following: `^/(?!cleartrust)`. This means: do not intercept URLs that include word `cleartrust`.

   For example, if before the change the file looked like this:

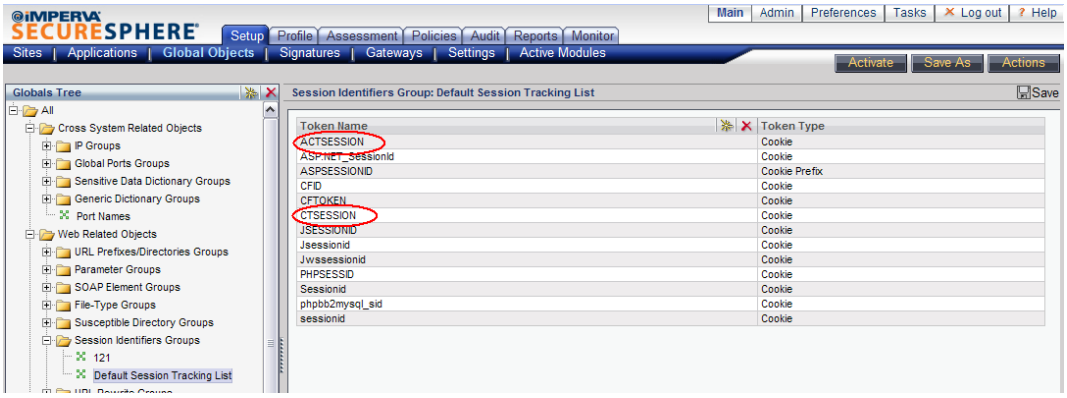
```
<VirtualHost 127.0.0.1:88>
  ServerName 10.3.220.22
  DocumentRoot /var/www/html/
  ProxyPreserveHost On
  RewriteEngine On
  RewriteRule ^/(.*) http://10.3.220.22/$1 [P]
  Header unset "WWW-Authenticate: NTLM"
  Header add WWW-Authenticate "Basic realm=SERVER-NAME"
</VirtualHost>
```

   Then it now should like this:

```
<VirtualHost 127.0.0.1:88>
  ServerName 10.3.220.22
  DocumentRoot /var/www/html/
  ProxyPreserveHost On
  RewriteEngine On
  RewriteRule ^/(?!cleartrust) (.*) http://10.3.220.22/$1 [P]
  Header unset "WWW-Authenticate: NTLM"
  Header add WWW-Authenticate "Basic realm=SERVER-NAME"
</VirtualHost>
```

6. Restart the httpd service by executing the following command:
   `service httpd restart`
7. The Access manager agent intercepts the connection and sets the user session with two session cookies CTSESSION and ACTSESSION. To enable SecureSphere to correctly learn the user's behavior you must add the cookies to the global object session identifier group.

   Either create a new group (duplicate) and add the new tokens, or use the default object. See the ***SecureSphere User Guide*** for details on adding tokens to Session Tracking Lists. Remember to associate the modified object with the protected service. You must add the following tokens as session cookies: CTSESSION and ACTSESSION.



8. To follow up on users in SecureSphere, you must configure AUT. The recommended way is to allow SecureSphere to learn the login and the action URLs and to then adjust decision rules according to the following considerations.

   An unsuccessful login is considered to be bad response code or redirection to either `/cleartrust/ct_logon_failed_en.html` or to `/cleartrust/ct_access_denied_en.html`

   Anything else (according to the default decision rule) is considered a successful login.

   See ***SecureSphere User Guide*** for details on how to configure Application User Tracking.



Note: In addition to Action URL, the `/cleartrust/ct_logon_failed_en.html` is also learned, because when a user is redirected to this page it contains form-based authentication. The decision rules for`/cleartrust/ct_logon_failed_en.html` are the same as above.

9. You must configure the Kernel Reverse Proxy to redirect client requests requiring authentication to run through the Apache Reverse Proxy. For more information, see Configuring KRP and Decision Rules on page 108.

Configuring Kernel Reverse Proxy and Apache Reverse Proxy on the Same Gateway

When Kernel Reverse Proxy and Apache Reverse Proxy are deployed together on the same SecureSphere gateway, the Kernel Reverse Proxy redirects matching traffic (based on URl and/or hostname) via the loopback interface to the Apache Reverse Proxy, which manipulates the session as required and communicates with the backend server.

For more information about this deployment, see Apache and Kernel Reverse Proxy on the Same Gateway on page 33.

To configure Kernel Reverse Proxy and Apache Reverse Proxy on the same SecureSphere gateway:

1. Configure the gateway as a Kernel Reverse Proxy, specifying that the outbound interface is the loopback interface.

   For information on how to configure Kernel Reverse Proxy, see Configuring Kernel Reverse Proxy on page 103.
2. Configure Apache Reverse Proxy on the same gateway, specifying that the ARP listens on the loopback interface.

   For information on how to configure Apache Reverse Proxy, see Configuring Apache Reverse Proxy on page 110.
3. Edit the Apache Reverse Proxy `httpd.conf` file and change the HTTP listener to listen to localhost on port 88 (for example, `listen 127.0.0.1:88`).
4. Edit `httpd.conf` to include protected hosts (virtual hosts).
5. Edit the Apache Reverse Proxy `nss.conf` file and comment out the line containing "`listen 443`" by inserting a `#` sign at the beginning of the line.

Switching Deployments

This section describes how to switch a SecureSphere appliance from one deployment mode to another, for example, from an inline gateway to a network monitor (sniffing) gateway, and includes:

- From a Onebox to a Gateway on page 118
- From a Gateway to a Onebox on page 118
- Changing the MX of a Gateway on page 118

Overview

It is not possible to convert a gateway appliance to an MX applicance, because of their different hardware configurations. However, a Onebox appliance can be reconfigured as a gateway only or as a management server only, and this reconfiguration can be later reversed.

From a Onebox to a Gateway

To convert an appliance from a Onebox to a gateway:

1. Start `impcfg`.
2. Select **Manage SecureSphere Server**.
3. Select **1) Deactivate server.**

From a Gateway to a Onebox

To convert an appliance from a gateway to a Onebox:

1. Start `impcfg`.
2. Select **Manage SecureSphere Server**.
3. Select **1) Activate server.**

Changing the MX of a Gateway

To change the MX of a gateway:

1. Delete the audit data from the gateway.
2. Start `impcfg`.
3. Select **Manage SecureSphere Gateway** > **Perform Actions** > **Stop gateway**.
4. Select **Manage SecureSphere Gateway** > **Perform Actions** > **Unregister gateway**.
5. On the gateway, start `impcfg`.
6. Select **Manage SecureSphere Gateway** > **Change server address / password** and specify the new MX.

CHAPTER 5

Installing Remote Agents

This chapter describes how to install the SecureSphere Remote Agent and configure it using the CLI.



Note: Information about AS/400 Remote Agent installation can be found in the ***SecureSphere User Guide***.

It includes the following sections:

Installing the Remote Agent on page 122
Uninstalling the Remote Agent on page 141
Upgrading the Remote Agent on page 143
Starting and Stopping the Remote Agent on page 144
Remote Agent Management Console on page 146
Diagnostic Tools on page 153
Prerequisite Tests for non-Windows Agents on page 155
Prerequisite Tests for non-Windows Agents on page 155
Supported Interfaces for the Gateway Listener on page 160
Advanced Agent Configuration on page 161
Command Line Scripting Language on page 168

Remote Agent Configuration Tasks

Installing and configuring the Remote Agent is a straightforward process, as outlined in the following table.



Note: DB2 Remote Agents on z/OS are installed and configured differently from other agents.

- For information on installing DB2 Remote Agents on z/OS, see Chapter 6, Installing SecureSphere Agent for DB2 z/OS.
- For information on configuring DB2 Remote Agents on z/OS, see the ***SecurerSphere User Guide***.

To install and configure the Remote Agent (most typical scenarios):

Remote Agent Configuration Task Checklist

Step		Action	Description	For more information, see
1		Obtain the latest version of the Remote Agent for your platform from the Imperva FTP site.	Make sure you download the correct agent installation file for your platform. Carefully review the Release Notes before continuing to the next step.	Preparing for Installation on page 122
2		Check the database or file server OS configuration.	Confirm that the proper version of the database software (including patches) is installed and that communications are correctly configured.	Preparing the Database on page 124
3		Configure the SecureSphere gateway.	Configure the gateway so that it can communicate with the Remote Agent.	Configuring the SecureSphere Gateway Before Installation on page 125
4		Install the Remote Agent.	Install the Remote Agent on the database and/or file server.	Installing the Remote Agent on page 127
5		Register the Remote Agent to the gateway.	Register the Agent to the gateway, so that it can start monitoring.	DB2 - AIX Post Installation Information on page 137
6		Configure the Remote Agent using the SecureSphere GUI.	Configure the Remote Agent in the **Agents** window in SecureSphere.	***SecureSphere User Guide***
7		Troubleshooting and control.	Use the management console for troubleshooting and control purposes.	Remote Agent Management Console on page 146



Note: SecureSphere supports Remote Agent versions earlier than 7.0, in a non-centrally managed mode. For more information about the earlier versions, see ***Remote Agents Configuration Guide.***

The configuration is composed of:

- the first time configuration wizard (registration)
- the SecureSphere GUI for most of the configuration
- the management console, used primarily for troubleshooting and control (start/stop)

Installing the Remote Agent

This section includes the following information:

- Preparing for Installation on page 122
- Configuring the SecureSphere Gateway Before Installation on page 125
- Installing the Remote Agent on page 127
- After Installing the Remote Agent on page 135
- First-Time Configuration Wizard on page 137
- Uninstalling the Remote Agent on page 141
- Upgrading the Remote Agent on page 143
- Starting and Stopping the Remote Agent on page 144
- DB2 - AIX Post Installation Information on page 137

Preparing for Installation

Before installing the Remote Agent, perform the following:

- Obtaining the Latest Version of the Remote Agent on page 122
- Verifying Prerequisites on page 123
- Preparing the Database on page 124



Note: In Unix and Unix-like systems, the bash shell must be available before installing the Remote Agent.

Obtaining the Latest Version of the Remote Agent

The latest version of the SecureSphere Remote Agent and the accompanying Release Notes are available on the Imperva FTP site. See the ***Remote Agent Release Notes***. for the exact location, which depends on the OS under which the Remote Agent will be running.



Note: For SUSE and OEL UEK, you must download two files:
- A `bsx` file, the self-extracting installation file.
- A `txt` file, which lists the SUSE kernel versions compatible with the remote agent.

For more information, see Special Considerations for SUSE and OEL UEK Platforms on page 130.

After downloading the Remote Agent **but before installing the Remote Agent**, carefully read the ***Remote Agent Release Notes***.

SharePoint

There are some special considerations for installing a Remote Agent for SharePoint monitoring.

1. The Remote Agent for SharePoint monitoring should be installed on only one of the WFEs. There is no need to install it on each of them.
2. When installing a Remote Agent for SharePoint monitoring, you must ensure that the Remote Agent and SecureSphere versions are the same, including the patch level. For example, if the SecureSphere version is 9.5 patch 1, then the Remote Agent version must also be 9.5 patch 1.
3. Installing and deploying a Remote Agent for SharePoint monitoring may take some time in large-scale environments. You should verify the status of the Remote Agent in the Agent Workbench before running the configuration wizard.

Verifying Prerequisites

Prerequisites are verified depending on the type of agent being installed.

- Verifying Prerequisites for non-Windows Agents on page 123
- Verifying Prerequisites for Windows Agents on page 124

Verifying Prerequisites for non-Windows Agents

The Remote Agent installation file is an executable which runs a pre-install script that verifies the system is ready for installing the Remote Agent and that all prerequisites are met. For more information, see Prerequisite Tests for non-Windows Agents on page 155.

The installation tool requires that the **df** program be in the defined **PATH** so that the available disk space can be determined. If this program is not in the **PATH**, then:

- If you are installing using the standard installation script, you will be asked to confirm that there is enough disk space available.
- If you are installing using the silent installation script, the installation will fail with an appropriate error message.



Note:
- You must install the Remote Agent from a user account which has write access to the **/usr/sbin** directory.
- Before running the pre-install script, make sure that the **/tmp** directory free space is at least twice the size of the package (**bsx**) file.

If the pre-install script discovers no problems, the Remote Agent is immediately installed.

You can also run only the pre-install script, in which case all tests performed by the pre-install script are run whether or not they fail and the script aborts before making any change to the system.

To run the pre-install script:



Note: The pre-install script is also run as part of the install script.

1. Make sure the Remote Agent installation file has executable permissions.
2. Run the Remote Agent installation file with the **-c** flag.

```
./ragent-<OS>-<OS version>-p<platform>-b<agent build>-r<agent release>
-k <file>  -c
```



Note: The **-k** <file> parameter is required only for SUSE installations. See Special Considerations for SUSE and OEL UEK Platforms below.

3. The following question appears:

```
Package root directory is /opt/imperva. "To change press 'n', otherwise
press 'y':"
```

Answer no ('n') only if you will install the Remote Agent in a location different from the default location. In this case, you must specify the pre-existing location (the installation procedure will not create directories).

SSH and Root Access

To complete the installation, you must have root user access to the DB host and SSH/Terminal connectivity.

HP-UX

For HP-UX, there are the following additional requirements:

- The HP-UX **`swinstall`** utility is used to install the Remote Agent. For **`swinstall`** to run properly, forward (IP address to hostname) and reverse (hostname to IP address) resolution must be enabled. Note that this is a general HP-UX issue, not an Imperva-specific issue.

Verifying Prerequisites for Windows Agents

The following prerequisites must be met before the agent can be installed.

Windows Update Installer Version

Confirm that the Windows Installer version is 3.1 V1 (3.1.4000.1823) or later.

To determine the version of the Windows Installer:

1. Locate the file **`MSI.DLL`** (this file is usually in **`C:\WINDOWS\SYSTEM32`**).
2. Right-click on the file name.
3. From the menu, select **Properties**.
4. Click the **Version** tab.
5. If the version number is not as required, use Windows Update to update Windows Installer to the latest version.

Winpcap



Note: This section is relevant only for database Remote Agents.

Winpcap is a packet capture application which is used by the Remote Agent to monitor network database traffic on external interfaces. If you are using the Remote Agent to monitor database traffic on external interfaces, you must install winpcap 4.1.2 or higher before you install the Remote Agent, because of issues with earlier versions of winpcap.

If you do not install winpcap 4.1.2 or higher, there is a possibility that the server will crash due to these winpcap issues, regardless of whether the Remote Agent is installed or running.

You can download the winpcap from the Imperva FTP server under the Remote Agent directory.

User Privileges

To complete the installation, you must have administrator user privileges on the database, file server or SharePoint server, as appropriate, and terminal connectivity.

SharePont Remote Agents



Note: Installing and deploying a SharePoint Remote Agent may take some time in large-scale environments. You should verify the status of the Remote Agent in the Agent Workbench before running the configuration wizard.

Preparing the Database



Note: This section is relevant only for database Remote Agents.

Many databases support several communication methods. In general, these fall into three categories: TCP/IP, TCP-local, and local inter-process communications (IPC).

The Remote Agent, installed on the database server machine, monitors database activity by listening on three channels:

channel	visibility to SecureSphere
external interfaces	This SQL/TCP activity can also be visible to a SecureSphere gateway.
loopback interface	This activity **is not visible** to a SecureSphere gateway, but it is visible to a Remote Agent.
inter-process communications (IPC)	This activity **is not visible** to a SecureSphere gateway, but it is visible to a Remote Agent. See the Release Notes for more information on the supported methods.

If the monitored database uses unsupported internal communication methods, you must configure the database to use the loopback for monitoring the local traffic. For example, if an Informix database is to be monitored locally, you must verify that its service is bound to the loopback interface.

If a SecureSphere gateway is also monitoring the database activity, the relevant Remote Agent should be configured so that it does not also monitor that same activity.

Configuring the SecureSphere Gateway Before Installation

The following configuration procedures must be performed on the Gateway before installing a Remote Agent:

- Configure the listeners. For more information, see Configuring Listeners on page 125.
- Configure routing. For more information, see Manage Remote Agent Related Routes on page 126.

Configuring Listeners

Remote Agent communicates with the SecureSphere gateway in two ways. It uses port 443 (this can be changed during the Gateway configuration) for registration, status, configuration and discovery of new data interfaces and a user defined port to transfer the captured DB activity. In most cases, this communication is over a secure TCP connection to a listener IP addrerss defined on the gateway. The listener is typically configured on the Gateway management IP address and is of type TCP.



Note:

- You can define multiple listeners of both types (TCP and UDP) on a gateway, and you can direct different Remote Agents to different listeners.
- Bridge and sniffing interfaces cannot be defined as TCP listener interfaces.
- A Remote Agent listener and a SecureSphere Agent for DB2 z/OS listener cannot be defined on the same port.

To configure a listener on SecureSphere gateway:

1. Start the `impcfg` CLI application on the gateway.
2. Select **Manage the SecureSphere gateway** from the Top menu.
3. Select **Manage remote agents**.
4. Select **Add a listener**.
5. Configure the listener parameters (see following table).

Listener Parameters

Option	Description
Listener type	The communication protocol between the Remote Agent and the gateway. Either TCP or UDP can be used. In most common scenarios, TCP is used and the listener is the end point for the Remote Agent communication. For more information on UDP mode, see Advanced Agent Configuration on page 161. Possible values: TCP | UDP
Listener IP address	The IP address to which the Remote Agent sends data. The IP address is assigned to the selected interface. Typically, you will select the IP address of the gateway's management interface. This IP address must be routable from the DB host. **Note:** Bridge and sniffing interfaces cannot be defined as TCP listener interfaces. If there is a firewall between the Remote Agent and the listener IP address, you must ensure that communication between them is allowed by the firewall. If the listener IP address is NATed, see Working with a NATed Listener on page 163
Listener IP mask	The network mask for the listener IP address. When gateway management IP address is used, enter its mask as defined on the gateway.
Listener port	The data port to which the Remote Agent sends its data. The port should be accessible and available. Choose a high port, for example 5555. If there is a firewall between the Remote Agent and the listener IP address, you must ensure that communication between them is allowed by the firewall. **Note:** Allowed values: 1 - 65355.
Listener interface	The physical gateway interface used for the listener. Typically, you will select the gateway's management interface. For more information, see Supported Interfaces for the Gateway Listener on page 160. **Note:** Bridge and sniffing interfaces cannot be defined as TCP listener interfaces. Possible value: eth5 | eth4 | eth3 | eth2 | eth1 | eth0
Virtual IP	When asked whether to enable virtual IP for the listener enter "n", unless you are using high availability gateways. For more information, see Working with High Availability on page 150. Possible value: y | n
Enable SSL	Enter "y" to encrypt traffic between the Remote Agent and its listener. Possible value: y | n

Manage Remote Agent Related Routes

The gateway listener and Remote Agent communicate over a secure TCP tunnel. In some environments, specific routes must be explicitly defined to enable the gateway to reach the DB host or file server IP address. SecureSphere version 6.0.6.6274 and above allow setting these routes using the **`impcfg`** application on the gateway.

To define Remote Agent-related routes on the gateway:

1. Start the **`impcfg`** CLI application on the gateway.
2. Select **Manage the SecureSphere gateway**.
3. Select **Manage remote agents**.
4. Select **Manage remote-agent related routes**.
5. Add or delete a route (see following tables):

Adding a Route

Option	Description
Will this be a virtual route, belonging to one of them?	Choose `n`, unless you are using high availability gateways. For more information, see Working with High Availability on page 150. Possible values: y| n.
Type	Define whether this route is per subnet or specific to host. Enter “host” unless you want the route to be valid for the whole network. Possible values: net | host.
Address	Available only when Type is “host”. Enter the IP address of the DB host.
Network	Available only when Type is “net”. Enter the IP address of the network base on the network subnet. For example, if the DB host’s IP address is 192.168.10.10 and its subnet mask is 255.255.0.0, the net IP address will be 192.168.0.0.
Subnet mask	Available only when Type is “net”. Enter the subnet mask of the network. Using the same example, the net subnet mask will be 255.255.0.0.
Gateway	The default gateway IP address used for the listener. Enter the default gateway IP address, which must be reachable from the listener subnet. If the listener IP address is the management IP address, you can choose a default gateway from the management subnet.
Device	The specific gateway physical interface to be used. If no interface is specified, the best available interface will be selected when routing.

Deleting a Route

Option	Description
Delete route	A list of available routes is displayed. Choose the route you wish to delete.

Agent routes are executed and added automatically when the gateway starts and are deleted automatically when gateway is stopped. The routes are maintained in the gateway’s `bootstrap.xml` file.

Installing the Remote Agent

The Remote Agent installation file is self-executable.

This section includes the following:

- Installing the Remote Agent on a non-Windows System on page 128
- Special Considerations for SUSE and OEL UEK Platforms on page 130
- Installing the Remote Agent on a Windows System on page 131
- Silent Installation Parameters on page 133

Installing the Remote Agent on a non-Windows System

The installation tool requires that the `df` program be in the defined `PATH` so that the available disk space can be determined. If this program is not in the `PATH`, then:

- If you are installing using the standard installation script, you will be asked to confirm that there is enough disk space available.
- If you are installing using the silent installation script, the installation will fail with an appropriate error message.

To install the Remote Agent on a non-Windows system:

1. Login to the machine as user `root`.



Note: If a previous version of the Remote Agent is installed on the machine, uninstall it, reboot and login again. For information about uninstalling a Remote Agent, see Uninstalling the Remote Agent on page 141.

2. Download and save the installation file, for example, to the `/tmp` directory.

   For information on obtaining the latest version of the Remote Agent software and release notes, see Obtaining the Latest Version of the Remote Agent on page 122.

   The installation file name is given in the Release Notes.
3. Verify that the installation file has executable permissions.
4. Install the Remote Agent using either:
   - 4.1 the standard installation script, which installs the Remote Agent, registers the Remote Agent by running the interactive configuration wizard, and then starts the Remote Agent (see Installing the Remote Agent on a Non-Windows System Using the Standard Script on page 128)
   - 4.2 a silent installation script, which installs the Remote Agent, registers the Remote Agent by running a non-interactive CLI command, and then starts the Remote Agent (see Silently Installing the Remote Agent on a non-Windows System on page 128)

Installing the Remote Agent on a Non-Windows System Using the Standard Script

To install the Remote Agent on a non-Windows system using the standard script:

1. Execute the following commands (assuming that you downloaded the installation file to the `/tmp` directory).

```
cd /tmp
<remote agent package full path> -k kabi_<n>.txt
```



Note: The `-k` parameter is required only for SUSE and OEL UEK installations. See Special Considerations for SUSE and OEL UEK Platforms below.

2. You are asked to specify a package root directory or to accept the default.
3. The package and system configurations are displayed and verification tests run.

   If any of the tests fails, the installation is aborted.

Silently Installing the Remote Agent on a non-Windows System

Silent installation enables you to install, register and start the Remote Agent without running the interactive configuration wizard.

To silently install the non-Windows agent:

1. Execute the following command:

```
<remote agent package full path> -n -d <remote agent directory>
```

where **remote agent directory** is the directory in which the remote agent will be installed.

2. Register the agent to the gateway by executing the following command:

```
<remote agent directory>/ragent/bin/cli --dcfg <remote agent directory>/ragent/
etc --dtarget <remote agent directory>/ragent/etc --dlog <remote agent
directory>/ragent/etc/logs/cli registration advanced-register registration-
type=<Primary | Secondary> ragent-name=<remote agent name>
tunnel-protocol=<TCP | UDP> site=mysite server-group="my server gropup"
gw-ip=<gateway IP> gw-port=<443>
manual-settings-activation=<Automatic | Manual>
monitor-network-channels=<Both | Local> password=<secure>
```

The parameters are explained in Silent Installation Parameters on page 133.

Alternatively, if you want to accept all the defaults (see Silent Installation Parameters on page 133), then execute the following command:

```
"<remote agent directory>/ragent/bin/cli [--dcfg <remote agent directory>/
ragent/etc --dtarget <remote agent directory>/ragent/etc --dlog <remote agent
directory>/ragent/etc/logs/cli] registration advanced-register ragent-
name=<remote agent name> gw-ip=<gateway IP>
```



Note: The parameters within the "[ ]" need to specified only if you installed the Remote Agent in a directory different from the default directory.

If you want to change one of the other parameters, you can add it to the command (see the full command above). For example:

```
"<remote agent directory>/ragent/bin/cli [--dcfg <remote agent directory>/
ragent/etc --dtarget <remote agent directory>/ragent/etc --dlog <remote agent
directory>/ragent/etc/logs/cli] registration advanced-register ragent-
name=<remote agent name> gw-ip=<gateway IP>
gw-port=<gateway management port>
```

3. Start the agent by executing the following command:

```
<remote agent directory>/ragent/bin/rainit start
```

EXAMPLE:

For example, the following commands silently install the remote agent, register the remote agent to the gateway at IP address 10.10.10.10, and then start the remote agent:

```
/tmp/agent.bsx -n -d /opt/imperva
/opt/imperva/ragent/bin/cli --dcfg /opt/imperva/ragent/etc --dtarget /opt/
imperva/ragent/etc --dlog /opt/imperva/ragent/etc/logs/cli registration
advanced-register registration-type=Primary ragent-name=`hostname' tunnel-
protocol=TCP gw-ip=10.10.10.10 gw-port=443 manual-settings-
activation=Automatic monitor-network-channels=Both password=secure
/opt/imperva/ragent/bin/rainit start
```

Special Considerations for SUSE and OEL UEK Platforms

SUSE and OEL UEK maintains several version of their OS, and service packs for each version. In addition, SUSE periodically releases updates to service packs, which sometimes include updated versions of the kernel.

Imperva SUSE and OEL UEK Remote Agents are specific to SUSE and OEL UEK versions and service packs, and are certified by Imperva as compatible with all kernel versions of a given service pack which were current at the time of the Remote Agent's release. When a new kernel version is released, Imperva tests the Remote Agent for compatibility with the new kernel.

Incompatibilties can arise in the following situations:

- You are trying to install a Remote Agent on a platform whose kernel is incompatible with that Remote Agent version.
- You are trying to start a Remote Agent on a platform whose kernel you have upgraded to a version incompatible with that Remote Agent version.

  In this case, the Remote Agent will not start, and a message will be displayed on the system console, and also in the log file **<installation directory>/ragent/etc/logs/agentstart.log**.

When Installing a SUSE or OEL UEK Remote Agent

The SUSE and OEL UEK Remote Agent installation consists of two files:

- Remote Agent self-extracting installation file (**bsx** file).
- Supported kernel versions file (**kabi_<n>.txt**), where **<n>** is the version number of the **kabi** file.

  This file is in the **\Downloads\SecureSphere_Agents\SUSE** directory, and applies to all SUSE and OEL UEK versions.

The pre-install script tests the compatibility of the Remote Agent with the kernel version by comparing the kernel version with the list in the supported kernel versions file. If the test fails, an error message is displayed and the installation is terminated.

If you receive this error message, download the correct file.

When Starting a SUSE OEL UEK Remote Agent

Each time the Remote Agent starts, it tests its compatibility with the kernel version. If the test fails, an error message is displayed on the system console (and written to the log file in the log file **<installation directory>/ragent/etc/logs/agentstart.log**) and the Remote Agent is not started. This can happen if you have upgraded the kernel to a version with which the Remote Agent is not compatible.

If you receive this error message, it may be that the kernel version is indeed supported, but because the supported kernel versions file is out-of-date, the Remote Agent fails the test. To solve this problem, proceed as follows:

1. Go to the Imperva FTP site.
2. Download the file **update_ragent_supported_suse_kernels_<n>.bsx** (where **<n>** is the version number) from the **\Downloads\SecureSphere_Agents\SUSE** directory.
3. Run the file you just downloaded.

This updates the `kabi_<n>.txt` file to the latest version.

4. Start the remote agent.
5. If the problem persists, contact suport.

   It may be that the kernel version to which you have upgraded is not compatible with the Remote Agent. Consult with Imperva support about what you should do next.

Installing the Remote Agent on a Windows System

To install the Remote Agent on a Windows system:

1. Login to the machine as administrator or as a user with administrator privileges.
2. Download and save the installation file.

   For information on obtaining the latest version of the Remote Agent software and release notes, see Obtaining the Latest Version of the Remote Agent on page 122.

   The installation file name is given in the Release Notes.
3. If a previous version of the Remote Agent is installed on the machine, then:
   - 3.1 Uninstall the previous version.

     For information about uninstalling a Remote Agent, see the ***SecureSphere User Guide***.
   - 3.2 For database remote agents only, if you are running MSSQL, then restart all MSSQL services.
   - 3.3 Login again.
4. Save the installation file on the local hard disk drive, preferably in a location that does not contain spaces in the path name.
5. Install the Remote Agent using either:
   - 5.1 The standard installation script, which installs the Remote Agent, registers the Remote Agent by running the interactive configuration wizard, and then starts the Remote Agent (see Installing the Remote Agent on a Windows System Using the Standard Script on page 131)
   - 5.2 A silent installation script, which installs the Remote Agent, registers the Remote Agent by running a non-interactive CLI command, and then starts the Remote Agent (see Silently Installing the Remote Agent on a Windows System on page 131)

Installing the Remote Agent on a Windows System Using the Standard Script

To install the Remote Agent on a Windows system using the standard script:

1. Run the MSI installation file you downloaded as administrator.

   If you do not have administrator privileges, proceed as follows:
   - 1.1 Open Windows Explorer and navigate to the MSI file (the installation file you saved in step 2.).
   - 1.2 Right-click the MSI file and select **Run as ...** from the menu.
   - 1.3 In the **Run As** window, select **The Following User**.
   - 1.4 Choose a user with administrator privileges.
   - 1.5 Enter the password.
   - 1.6 Click **OK**.

   Otherwise, run the Remote Agent installation file by executing the following command:

```
<remote agent package installation file>.msi
```

Silently Installing the Remote Agent on a Windows System

Silent installation enables you to install, register and start the Remote Agent without running the interactive configuration wizard.

To silently install the Windows Remote Agent:

1. Execute the following command:

```
msiexec /i "<remote agent package full path>\<package name.msi>" NOSCRIPT=true
     /quiet
```

   Replace `<remote agent package full path>` with the full path name of the directory, and `<package name.msi>` with the name of the installation file, and enclose the whole string in quotes.

2. Register the Remote Agent to the gateway by executing the following command:

```
"<remote agent directory>\RemoteAgentCli.exe" --dcfg "<remote agent directory>"
--dtarget "<remote agent directory>" --dlog "<remote agent directory>\logs\cli"
registration advanced-register registration-type=<Primary | Secondary>
is-db-agent=<true | false> is-fam-agent=<false | true> is-sp-agent=<false |
true> ragent-name=<remote agent name> tunnel-protocol=<TCP | UDP> site=mysite
server-group="my server group" gw-ip=<gateway IP>
gw-port=<443> manual-settings-activation=<Automatic | Manual>
monitor-network-channels=<Both | Local> password=<secure>
```

   The parameters are explained in Silent Installation Parameters on page 133.

   Alternatively, if you want to accept all the defaults (see Silent Installation Parameters on page 133), then execute the following command:

```
"<remote agent directory>\RemoteAgentCli.exe" [--dcfg "<remote agent
directory>" --dtarget "<remote agent directory>" --dlog "<remote agent
directory>\logs\cli"] registration advanced-register ragent-name=<remote agent
name> gw-ip=<gateway IP>
```



Note: The parameters within the "[ ]" need to specified only if you installed the Remote Agent in a directory different from the default directory.

   If you want to change one of the other parameters, you can add it to the command (see the full command above). For example:

```
"<remote agent directory>\RemoteAgentCli.exe" [--dcfg "<remote agent
directory>" --dtarget "<remote agent directory>" --dlog "<remote agent
directory>\logs\cli"] registration advanced-register ragent-name=<remote agent
name> gw-ip=<gateway IP>
gw-port=<gateway management port>
```

3. Start the agent by executing the following command:

```
sc start "SecureSphereRemoteAgent"
```

EXAMPLE:

For example, the following commands install the Remote Agent, silently register the Remote Agent to the gateway at IP address 10.10.10.10, and then start the remote agent:

```
msiexec /i C:\Program Files\Imperva\RemoteAgent NOSCRIPT=true  /quiet
"C:\Program Files\Imperva\RemoteAgent\RemoteAgentCli.exe" --dcfg "C:\Program
Files\Imperva\RemoteAgent" --dtarget "C:\Program Files\Imperva\RemoteAgent" --
dlog "C:\Program Files\Imperva\RemoteAgent\logs\cli" registration
advanced-register registration-type=Primary is-db-agent=true
is-fam-agent=false is-sp-agent=false ragent-name=MyAgent tunnel-protocol=TCP
site=mysite server-group="my server group" gw-ip=10.10.10.10 gw-port=443
manual-settings-activation=Automatic monitor-network-channels=Both
password=secure
sc start "SecureSphereRemoteAgent"
```

Silent Installation Parameters

The following table lists and explains the parameters for silent installations.

Silent Agent Registration Parameters

Parameter	Description
Windows: `--dcfg "<remote agent directory>"`	`<remote agent directory>` is normally the same directory in which the agent is installed.
non-Windows: `--dcfg <remote agent directory>/ragent/etc`	
Windows: `--dtarget "<remote agent directory>"`	
non-Windows: `--dtarget <remote agent directory>/ragent/etc`	
Windows: `--dlog "<remote agent directory>\logs\cli"`	
non-Windows: `--dlog <remote agent directory>/ragent/etc/logs/cli`	
`registration advanced-register`	Required.
`registration-type`	Specify "`Primary`" or "`Secondary`". See Do you wish to register Remote Agent to a secondary gateway on page 140. **Default:** `Primary`

Silent Agent Registration Parameters

Parameter	Description
Windows Only: `is-db-agent`	Specify `true` for database agents. **Default:** `true`
Windows Only: `is-fam-agent`	Specify `true` for file agents. **Default:** `false`
Windows Only: `is-sp-agent`	Specify `true` for SharePoint agents. **Default:** `false`
`ragent-name`	The name of the agent, as it will appear in the SecureSphere GUI. See Enter the Remote Agent name on page 138.
`tunnel-protocol`	Specify TCP or UDP. See Choose TCP or UDP communication on page 139. **Default:** `TCP`
`site`	Specify the Remote Agent's site in SecureSphere. If you specify `site`, then you must also specify `server group`. `site` is case-sensitive, embedded spaces are allowed (but you should then enclose the name in quotes, for example, "Big Site"), and leading and trailing spaces are not stripped out. **Default:** None
`server-group`	Specify the Remote Agent's server group (within the site). If you specify `server-group`, then you must also specify `site`. `server-group` is case-sensitive, embedded spaces are allowed (but you should then enclose the name in quotes, for example, "Server GroupA"), and leading and trailing spaces are not stripped out. **Default:** None
`gw-ip`	The IP address of the gateway to which the agent will be registered. See Enter the Management Gateway listener IP address on page 139.

Silent Agent Registration Parameters

Parameter	Description
`gw-port`	The management listener port number on the gateway. See Enter the Management Gateway listener port on page 139. **Default:** `443`
`manual-settings-activation`	Specify `Manual` or `Automatic`. **Default:** `Automatic` See Choose manual settings activation (configuration updates) on page 139.
`monitor-network-channels`	Specify `Local` or `Both`. The type of traffic to be monitored: • `Local` - local traffic only • `Both` - local and external traffic **Default:** `Both`
`password`	See Enter the Gateway login password on page 140. **Default:** `secure`

After Installing the Remote Agent

This section reviews comments related to post agent installation and includes:

- Data Interface Discovery and Configuration on page 136
- MSSQL Post Installation Information on page 137
- Oracle - Windows Post Installation Information on page 137
- DB2 - AIX Post Installation Information on page 137
- AIX Post Installation Information on page 137

Data Interface Discovery and Configuration

The Remote Agent does not automatically disover data interfaces for all OS/DB/interface type combinations, so in some cases you will have to manually configure the interfaces.

The table below lists the data interfaces automatically discovered by the Remote Agent, and those which the user must manually configure.

Table 1 Automatic Data Interface Discovery

OS	Database	Interfaces
Automatic Discovery		
Unix-like	**Oracle**	TCP external
		TCP local
		IPC
		BEQ
	Sybase	TCP external
		TCP local
Windows	**MSSQL**	TCP external
		TCP local
		MSSQL IPC (shared memory / named pipes)
Windows Itanium	none	none
Manually Configured		
Windows	**Oracle**	TCP external
		TCP local
		IPC
		BEQ
	All Other Supported Databases	TCP external
		TCP local
Unix-like	**DB2**	TCP external
		TCP local
		shared memory
	All Other Supported Databases	TCP external
		TCP local

Contact your DBA for information about the data interfaces on your database server.

For more information on configuring data interfaces, see the SecureSphere User Guide.

MSSQL Post Installation Information

If you have done one of the following:

- upgraded the Remote Agent to a newer version
- downgraded the Remote Agent to a previous version

then you must restart the MSSQL Server. Otherwise, the newly installed Remote Agent will continue to use the old version of `ipc.dll`.

Oracle - Windows Post Installation Information

If you have upgraded the Windows Remote Agent , you must restart the Oracle Server.

DB2 - AIX Post Installation Information

If you are connecting to DB2 locally over shared memory, then you must restart all DB2 database instances after the first time you start the Remote Agent. There is no need to reboot the machine.

AIX Post Installation Information

If you wish to monitor local connection over shared memory to DB2 , then you must restart the login servers (SSH, Telnet, Rlogin) after the first time you start the Remote Agent.

There is no need to reboot the machine.

First-Time Configuration Wizard

The configuration wizard guides you through the initial configuration of the Imperva agent. The configuration wizard starts automatically after the Remote Agent finishes installing.

You should use the configuration wizard only for the first time configuration. You can later make changes to the configuration using the Remote Agent Management Console. For more information, see Remote Agent Management Console on page 146.

To run the configuration wizard again at another time:

1. Execute the following command:
   - **In non-Windows**: `<base dir>/ragent/bin/racli`

     The default `<base dir>` is `/opt/imperva`
   - **In Windows**: `<base dir>\RemoteAgent\StartCli.bat`

     The default `<base dir>` is `C:\Program Files\Imperva/`
2. Select option 1.

   The configuration wizard uses the following conventions:

Configuration Wizard Conventions

Convention	Meaning
`<y>`	confirm
`<d>`	discard and continue
`<n>`	continue
`<s>`	save

Configuration Wizard Conventions (continued)

Convention	Meaning
<q>	quit (discard un-saved settings)
<j>	jump to previous level
[value]	the default value to be used
<h>	help

The log file for the configuration wizard errors in non-Windows systems is:

<base dir>/ragent/etc/clilog/CliLog.html

The default is **<base dir>** is **/opt/imperva**

The log file for the configuration wizard errors in Windows systems is:

<base dir>\RemoteAgent\CliLog.html

The default **<base dir>** is **C:\Program Files\Imperva**

The configuration wizard will guide you through a series of questions in the order given below. If you are not certain about the configuration suggested by the configuration wizard, choose the default option. You can always reconfigure it later using the Remote Agent management console. See Remote Agent Management Console on page 146 for more information.

Registering the Remote Agent to a SecureSphere Gateway



Note: Version 7.0 and higher agents work with only with SecureSphere Gateway versions 7.0 and higher.

To complete the initial configuration wizard, you must register your agent to the SecureSphere Gateway.

Registration is the process by which the Remote Agent identifies itself to the gateway. When registering the Remote Agent to the gateway listener, the listener defines the listener port in the Remote Agent configuration file and knows from which Remote Agent to expect traffic.

You are given the choice of two registration options: quick (typical) registration, where most parameters are defined to their typical values, and advanced registration, where you must explicitly define each parameter.

If you decide to exit at this point, you can register later using the Remote Agent management console. See Remote Agent Management Console on page 146 for more information.

Agent Registration Steps

Registration Step	Description
Which type of traffic should be monitored? **Note:** This option is available only for Windows Remote Agents.	The type of traffic to be monitored: 1) **Database**: Only database traffic will be monitored. **2) File**: Only file traffic will be monitored. **3) Both**: Both database and file traffic will be monitored.
Enter the Remote Agent name	Enter a name for the Remote Agent. This name will be used in the SecureSphere GUI to identify the Remote Agent. Enter alphanumeric characters.

Agent Registration Steps

Registration Step	Description
Enter SecureSphere site name	Enter the name of the site to which to attach the Remote Agent. Leave the site name empty if you are not sure of it at this point. You can always attach the Remote Agent to a site later using the SecureSphere GUI. Note that the site name is case-sensitive, embedded spaces are allowed, and leading and trailing spaces are not stripped out.
Enter SecureSphere server group name	Enter the name of the server group (in the above site) to which to attach the Remote Agent. Leave the server group name empty if you are not sure of it at this point or if you did not enter a site name. You can always attach the Remote Agent to a server group later using the SecureSphere GUI. Note that the server group name is case-sensitive, embedded spaces are allowed, and leading and trailing spaces are not stripped out.
Choose TCP or UDP communication	This option defines the communication mode that the Remote Agent uses to send captured DB activity to the gateway. The registration itself is always done using TCP. Most common scenarios use TCP communications.
Enter the Management Gateway listener IP address	Enter the gateway management listener IP address, as defined in the SecureSphere gateway listener configuration (see Managing Remote Agents on page 76). This is the IP address with which the Remote Agent registers, typically the SecureSphere gateway's management IP address. **Note:** Bridge and sniffing interfaces cannot be defined as TCP listener interfaces.
Enter the Management Gateway listener port	The gateway port used for registration. After successful registration, the listener configures the Remote Agent configuration file with the high port used for the TCP tunnel, as defined on the gateway when configuring the listener (see Managing Remote Agents on page 76). Use 443 as the port, unless it has been changed through the gateway configuration manager (`impcfg`).
Choose manual settings activation (configuration updates)	Manually activate of Remote Agent settings. The following options are available: • **Manual**: The configuration changes performed using SecureSphere are manually approved by the user before they are applied to the Agent. • **Automatic**: All the configuration changes performed using SecureSphere are automatically applied to the Remote Agent. **Default**: Automatic.
Monitor only local activity, or monitor both local activity and network traffic	**Note:** This parameter is relevant for database Remote Agents only. If external traffic is monitored by a SecureSphere gateway, the remote agent should monitor only local traffic so as to prevent the remote agent and the gateway reporting the same traffic. The following options are available: • **Local**: Monitor only local traffic. • **Both**: Monitor both local and external traffic. When ignoring traffic on external data interfaces, SecureSphere automatically ignores new TCP data interfaces. This can be overridden manually in the **Settings** tab of the **Agent** window. For more information, see the ***SecureSphere User Guide***.

Agent Registration Steps

Registration Step	Description
Enter the Gateway login password	The password of the user “imperva” on the gateway. Use “secure” as the password, unless this has been changed using `impcfg` on the gateway.
Do you wish to register Remote Agent to a secondary gateway	If you want to define a high availability configuration, then you must configure a secondary gateway in addition to the primary gateway. **Note:** The secondary gateway must be in the same gateway group as the primary gateway. If it is not, the registration process will fail. To register the Remote Agent to a secondary gateway, you must go through this same configuration process on the secondary gateway.

Upon successful registration, the following message appears: “The agent was successfully registered to Gateway.”

If you receive an error message, see Remote Agent Error Messages on page 153 for more information.

Uninstalling the Remote Agent



Note: These instructions refer to uninstalling Version 8.5 and higher Remote Agents. It does not include information about AS/400 and z/OS Remote Agents.
For uninstalling a previous version, see the ***SecureSphere User Guide*** for that version.

This section includes:

Uninstalling the Remote Agent on a non-Windows System on page 141
Uninstalling the Remote Agent on a Windows System on page 142

Uninstalling the Remote Agent on a non-Windows System

To uninstall the Remote Agent software on non-Windows system:

1. Stop the Remote Agent (see Starting and Stopping the Remote Agent on page 144).
2. Execute: the following command:

```
<base dir>/bin/uninstall
```

   where **<base dir>** is the directory in which the Remote Agent is installed.

3. Follow the on-screen instructions.

   If the uninstall completes successfully, the Remote Agent was uninstalled. However, it is possible that the Remote Agent driver was not completely removed because it is being used by other processes. If this happens, a message will be displayed that the driver has not been removed.

   If the driver was not removed, there is nothing you need to do. The presence of the driver after the Remote Agent has been uninstalled has no effect on the system. The driver code is not run, and in Remote Agent versions 8.0 higher, all the memory used by the driver is returned to the system. In Remote Agent versions prior to version 8.0, the driver's memory is not returned to the system, but otherwise the driver does not affect performance.

   Post-Version 8.5 drivers will be removed automatically after the next reboot (except for HP-UX 11.11).

   If the version of the uninstalled Remote Agent is earlier than Version 8.5 P2 and for all HP-UX 11.11 Remote Agents (whatever the version), you must manually delete the driver after the next reboot with the **kragent_unload** command.

   - Version 8.5 and higher: **<base dir>/ragent/sbin/krg_<version number>/kragent_unload**
   - Pre-Version 8.5: **<base dir>/ragent/sbin/kragent_unload**

After Uninstalling the Remote Agent on a non-Windows System

In general, you do not need to reboot the database server after uninstalling the Remote Agent, with the exceptions listed in the following paragraphs.

AIX

After Uninstalling a Version 9.0 or Higher Remote Agent

You can re-install the same version without rebooting the database server. If you want to install a pre-version 9.0 Remote Agent, you must reboot the database server.

After Uninstalling a Pre-version 9.0 Remote Agent

The uninstall process will ask you to reboot the database server. If you plan to install version 9.0 or higher Remote Agent, ignore the message. You do not have to reboot the datbase server.

EXAMPLE:

If you uninstall a version 8.5 Remote Agent and plan to install a version 8.5 Remote Agent, you must reboot the database server after the uninstall.

However, if you uninstall a version 8.5 Remote Agent and plan to install a version 9.0 Remote Agent, you do not have to reboot the database server, even though a message is displayed telling you that you must reboot.

Linux, Solaris and HP-UX

The driver will be automatically removed after the next reboot (except for HP-UX 11.11 PA-RISC; see below).

If you uninstall the Remote Agent and plan to re-install the same Remote Agent version you just uninstalled, then you must reboot the database server after uninstalling the Remote Agent and before re-installing the Remote Agent.

HP-UX 11.11 PA-RISC

The driver will not be automatically removed after the next reboot. To remove the driver, run the following command immediately after the reboot, where:

- `<base dir>` is the directory in which the Remote Agent was installed. The default directory is `/opt/Imperva`
- `<version number>` has the format X_Y_0_BN (for example, `8_5_0_0013`) where:
  - X is the major version number (for example, 8)
  - Y is the minor version number (for example, 5)
  - BN is the four-digit build number, exactly as it appears in the name of the Remote Agent installation file.

Remote Agent Version	To remove the driver, run the following command immediately after the reboot:
8.5	`<base dir>/ragent/sbin/krg_<version number>/kragent_unload`
pre-8.5	`<base dir>/ragent/sbin/kragent_unload`

Uninstalling the Remote Agent on a Windows System

To uninstall the Remote Agent software on a Windows system:

1. Stop the Remote Agent (see Starting and Stopping the Remote Agent on page 144).
2. Using the Windows Add/Remove Program Control Panel applet, uninstall **Imperva SecureSphere remote agent software**.

To silently uninstall the Remote Agent software on a Windows system:

1. Execute the following command:

```
msiexec /x <remote agent package full path> NOSCRIPT=true /quiet
```

Upgrading the Remote Agent

To upgrade the Remote Agent, you must first uninstall the Remote Agent and then install the new version.



Note: These instructions refer to upgrading to Version 8.5 and higher Remote Agents. For upgrading to previous versions, see the ***SecureSphere User Guide*** for that version.

This section includes:

- Upgrading the Remote Agent on a non-Windows System on page 143
- Upgrading the Remote Agent on a Windows System on page 143

Upgrading the Remote Agent on a non-Windows System

To upgrade the Remote Agent on a non-Windows system:

1. Uninstall the Remote Agent.

   For information about uninstalling the Remote Agent, see Uninstalling the Remote Agent on a non-Windows System on page 141.

   Depending on the OS and the version number of the Remote Agent you just uninstalled, you may or may not have to reboot the database server after uninstalling the Remote Agent. For more information, see After Installing the Remote Agent on page 135.

2. Install the new Remote Agent.

   For information about installing the Remote Agent, see Installing the Remote Agent on a non-Windows System on page 128.

Upgrading the Remote Agent on a Windows System

To upgrade the Remote Agent on a Windows system:

1. Uninstall the Remote Agent.

   For information about uninstalling the Remote Agent, see Uninstalling the Remote Agent on a Windows System on page 142.

2. Install the new version of the Remote Agent.

   For information about installing the Remote Agent, see Installing the Remote Agent on a Windows System on page 131.

Starting and Stopping the Remote Agent

This section reviews topics relating to the starting and stopping of the Remote Agent and includes the following subjects:

- Starting and Stopping the Remote Agent from the Management Console on page 144
- Starting the non-Windows Remote Agent from the Command Line on page 144
- Stopping the non-Windows Remote Agent from the Command Line on page 145
- Starting the Windows Remote Agent from the Command Line on page 145
- Stopping the Windows Remote Agent from the Command Line on page 145

After the initial configuration wizard completes successfully, you have the option of starting the Remote Agent. If you wish to start the Remote Agent at a different time, exit the configuration wizard and then start the Remote Agent from either the Remote Agent Management Console or from the command line.

For more information about the Remote Agent Management Console, see Remote Agent Management Console on page 146.



Note: The Remote Agent cannot be started or stopped from the SecureSphere GUI, only from the Remote Agent Management Console or from the OS command line.

Starting and Stopping the Remote Agent from the Management Console

To stop, start or restart the Remote Agent:

1. From the top level menu, select **Perform Actions (Start/Stop/Restart)**.
2. Choose one of the above options (**Start/Stop/Restart**).

Starting the non-Windows Remote Agent from the Command Line

To start the Remote Agent:

1. Execute one of the following commands:

```
<remote agent directory>/ragent/bin/rainit start
```

```
<remote agent directory>/ragent/bin/cli actions start
```

Stopping the non-Windows Remote Agent from the Command Line

To stop the Remote Agent:

1. Execute one of the following commands:

```
<remote agent directory>/ragent/bin/rainit stop
```

```
<remote agent directory>/ragent/bin/cli actions stop
```

Starting the Windows Remote Agent from the Command Line

To start the Remote Agent:

1. Execute the following command:

```
"<remote agent directory>\RemoteAgentCli.exe" actions start
```

Stopping the Windows Remote Agent from the Command Line

To stop the Remote Agent:

1. Execute one of the following commands:

```
"<remote agent directory>\RemoteAgentCli.exe" actions stop
```

Remote Agent Management Console

The Remote Agent Management Console is a tool designed to help you perform additional actions relevant to the Remote Agent, which are not available in the SecureSphere GUI.

From the menu it is possible to control the Remote Agent (register/un-register, start, stop etc.), change agent settings and even troubleshoot.

This section describes how to use the Remote Agent Management Console and includes the following information:

- Remote Agent Management Console Conventions on page 146
- Starting the Remote Agent Management Console on page 147
- Registering the Remote Agent to the Gateway on page 147
- Starting and Stopping the Remote Agent on page 144
- Activating Settings Manually on page 148
- Agent Information Displayed in the Console on page 149
- Agent Troubleshooting Using the Management Console on page 149

Remote Agent Management Console Conventions

The Remote Agent management console uses the following conventions:

<c>	confirm
<d>	discard and continue
<s>	save
<q>	quit (discard un-saved settings)
<j>	jump to previous level
<r>	jump to root menu (top level)
[value]	the default value to be used
A | D | C	this configuration item has been added (**A**), deleted (**D**) or changed (**C**)
Esc	exit command execution
<h>	help



Note:
- Configuration changes are not automatically saved. You must save them explicitly before exiting.
- Changes take effect only after the Remote Agent is restarted.

non-Windows Agents

The log file for the Remote Agent management console errors is:

<base dir>/ragent/etc/logs/cli/cli.html

The default **<base dir>** is **/opt/imperva**

Windows Agents

The log file for the Remote Agent management console errors is:

<base dir>\RemoteAgent\logs\cli\cli.html

The default **<base dir>** is **C:\Program Files\Imperva**

Starting the Remote Agent Management Console

To start the Remote Agent Management console in a non-Windows system:

1. Run the following command:

   `./<base dir>/ragent/bin/racli`

The default `<base dir>` is `/opt/imperva`

To start the Remote Agent Management console in Windows:

1. Run the following command:

   `<base dir>\RemoteAgent\StartCli.bat`

The default `<base dir>` is `C:\Program Files\Imperva`

2. Choose 2 for Menu mode.

Registering the Remote Agent to the Gateway

To register the Remote Agent to a listener on a SecureSphere gateway:

1. Choose **Manage Remote Agent Registration** from the top level menu.
2. Choose **Register the Remote Agent to Gateway** and set the following parameters:

Choose the registration type	Select if the registration type is Primary or Secondary. When the connection with the primary gateway is lost the Agent communicates with the secondary gateway. If you choose secondary registration without doing primary registration first, then the registration fails immediately with an appropriate error message.
Choose TCP or UDP communication	Choose the desired communication protocol between the Remote Agent and SecureSphere gateway based on the listener configuration on the Gateway and your topology. the Remote Agent captures database activity and dispatches it to the gateway via a TCP tunnel directly to the listener or via a UDP tunnel. For more information on UDP tunnels, see UDP Tunnel Mode on page 161. Registration, configuration updates, status messages, and auto discovery results are always performed using TCP. UDP can be used only for the data interface.
Enter the Remote Agent name	Enter a descriptive name for the Remote Agent. This is the name that will appear in the SecureSphere UI. Allowed values: alphanumeric characters, and the number of characters must be between 1 and 80.

Choose manual settings activation (configuration updates)	Enables manual activation of agent's settings. The following options are available: • **False**: All the configuration changes performed using SecureSphere are automatically applied to the Agent. • **True**: The configuration changes performed using SecureSphere are manually approved by the user before they are applied to the Agent. **Default**: False.
Choose to ignore external (TCP) interfaces	Enables ignoring the traffic that arrives from outside to the specific database in addition to the local traffic. In this case the Agent monitors all the traffic that is usually monitored by the Gateway. Here you need to decide if the default value is Enabled/Disabled.
Enter the Gateway listener IP address	Enter the gateway listener IP address as defined in the SecureSphere gateway listener configuration. This is the IP address that the Remote Agent registers with. If TCP is used as communication type, this IP address is used as the end point for the TCP tunnel. **Note:** Bridge and sniffing interfaces cannot be defined as TCP listener interfaces.
Enter the Gateway listener port	This is the port used for registration. Upon successful registration, the gateway configures the Remote Agent with the listener high port used for the tunnel. Use port 443, unless this was changed on the gateway (using the gateway configuration manager).
Enter the Gateway login password	Use "secure" as password, unless this was changed on the gateway (using the gateway configuration manager). This is the password of user "imperva" on the gateway.
Save pending changes	All changes must be confirmed and saved before registration continues. Note: All changes in the configuration take effect only after restarting the Remote Agent.

At the end of this process, the Remote Agent registers with the gateway and the following message is displayed: **The Remote Agent was successfully registered to Gateway**.

If a different message appears see Remote Agent Error Messages on page 153 for more information.

Upon successful registration, the Agent appears in the GUI, and further configuration can be done from there.



Note: If you remove a gateway, then before you can re-register the agent to the gateway, you must remove the secondary gateway as well.

Activating Settings Manually

When the Manual Settings Activation option is enabled, see Registering the Remote Agent to the Gateway on page 147, you need to activate manually the settings performed in the Agents window in the GUI. Once the configuration is done in the Agents window, you need to apply it manually in the Agent's console.

Before applying the settings, check if there are pending changes, see Agent Information Displayed in the Console on page 149.

To activate settings manually:

- From the top level menu, select **Activate Settings**.

Agent Information Displayed in the Console

The following information is displayed above the menus in the Console:

- **Release Number**: Agent's release number.
- **Registration Status**: Shows if the Agent is registered or not. The values are True - registered, False - not registered.
- **Remote Agent Status**: The current status of the Agent, the values can be Stopped or Running.
- **Pending Configuration Update**: Indicates if there are configuration changes that should be manually activated, see Activating Settings Manually on page 148, the values are True/False.

Agent Troubleshooting Using the Management Console

The troubleshooting menu allows collecting logs, watching the full agent configuration and its counters.

To troubleshoot the Remote Agent:

1. Choose "Troubleshooting" from the top menu.

The sub menu includes 4 options:

- Change Log Level
- Show Counters

Show Counters

This option displays the Remote Agent user space counters, information which is useful for debugging, and is located in:

non-Windows

```
<base dir/ragent/etc/logs/ragent/ragent_log.htm.counter.html
```

Windows

```
<base dir>\RemoteAgent\logs\ragent\ragent_log.htm.counter.html
```

Counters include information on the Remote Agent and OS activity. Example of such information: agent start time, OS CPU usage, agent user space cpu usage, number of packets that were received from interface and so on. Counter information is meaningful to the Imperva support team and should be printed if requested.

Working with High Availability

To work in the high availability mode, agents can be registered to two gateways. This is the preferred option.



Note: In High Availability configurations, both gateways must be in the same gateway group.

If you are using an older version of agents, you can achieve high availability by having two gateways configured with the same virtual IP address to which the Agent is reporting to. SecureSphere allows you to configure two listeners in high availability mode. Using the VRRP protocol, it is possible to configure the listeners to use one virtual IP, which is used as the TCP tunnel end point. One of the listener IP addresses acts as a master and processes the traffic, while the other IP address acts as backup. If the master fails, its role is then taken by the backup. This configuration ensures that the Remote Agent traffic is always processed and reported to the management server.



Note: The Remote Agent buffering feature ensures that traffic is not lost if the Remote Agent cannot communicate with the gateway listener.

For more information on high availability in UDP mode, see High Availability in UDP Mode on page 162.

To complete the configuration, perform the following tasks:

1. Configure the gateway listeners to use VRRP (see Configuring the Gateways to Operate in the HA Mode with Agents on page 150).
2. Configure the Remote Agent to register with both gateways (see Configuring the Remote Agent to Operate in the HA Mode on page 152).

Configuring the Gateways to Operate in the HA Mode with Agents

To configure the gateways:

1. Configure a listener on the SecureSphere gateway. See Configuring Listeners on page 125 for more information.
2. To the question “Do you want to use VRRP for this listener?”, enter “`y`”.
3. Answer the remaining the questions according to the table below:

Virtual instance name	The name of the VRRP circuit, which must be identical for both gateways. Permitted characters are alphanumeric and underscore.
Virtual IP address	The virtual address for VRRP, which must be identical for both gateways.
Virtual IP mask	The virtual IP mask, which must be identical for both gateways.
Virtual router ID	The ID of the VRRP circuit, which must be identical for both gateways. This must be a number between 1 and 255.
Virtual router mode	The virtual router mode MASTER or BACKUP. Only one of the gateways is assigned the MASTER status.
Enable SSL	Set if the Remote Agent will send its data encrypted. Possible value: y | n



Note: You must use the same listener port on both gateways. See Configuring the SecureSphere Gateway Before Installation on page 125.

To define a VRRP agent related route on the gateways:

1. SSH to the gateway.
2. Login as user secure.
3. Select **Manage the SecureSphere gateway**.
4. Select **Manage remote agents**.
5. Select **Manage remote-agent related routes**.

Adding Routes

Option	Description
Will this be a virtual route, belonging to one of them?	Choose yes. The route will be associated with the Virtual IP. Possible value: y| n
Which virtual instance	Enter the virtual instance name to which the route will apply.
Type	Define whether this route is per subnet or specific to host. Possible value: net | host Enter “host” unless you want the route to be valid for the whole network.
Address	Available only when Type host is selected. Enter the IP address of the DB host.
Network	Available only when Type net is selected. The IP address of the network base on the network subnet. For example DB host IP address is 192.168.10.10 and its subnet mask 255.255.0.0, the net IP address will be 192.168.0.0.
Subnet mask	Available only when Type net is selected. The subnet mask of the network. Based on the example above net subnet mask will be 255.255.0.0
Gateway	Specify the default gateway IP address which is used for the listener. The default gateway IP must be from the listener subnet. If the listener IP address is the management IP address, you can choose a default gateway from the management subnet.
Device	Specify specific gateway physical interface to use or Enter for none. If none is selected, the best available interface is selected when routing.

Deleting Routes

Option	Description
Delete route	List of available routes is presented. Choose the route you wish to delete.

Agent routes are executed and added automatically when gateway starts and are deleted automatically when gateway is stopped. The routes are kept in the gateway `bootstrap.xml` file.

Configuring the Remote Agent to Operate in the HA Mode



Note: This section is relevant only for pre-version 7.0 Remote Agents.

Configure the Remote Agent according to the configuration guides outlined throughout this document. When done, register the Remote Agent with both of the version 6.0 gateways.

To configure the Remote Agent:

1. Configure the Remote Agent.
2. Save the configuration.
3. Register the Remote Agent with primary gateway private listener IP (see Registering the Remote Agent to the Gateway on page 147).
4. Register the Remote Agent again, now with secondary gateway private listener IP (see Registering the Remote Agent to the Gateway on page 147).
5. Start the Remote Agent (see Starting and Stopping the Remote Agent on page 144).
6. If the Remote Agent registers with a listener that uses VRRP, the gateway updates the Remote Agent configuration file with the virtual IP address, as the TCP tunnel destination IP address.

Diagnostic Tools

This section includes the following information:

- Remote Agent Logs on page 153
- Remote Agent Error Messages on page 153
- Maintenance Tasks on page 154
- Remote Agents in a Hypervisor (Virtualized) Environment on page 154

Remote Agent Logs

The Remote Agent maintains several logs.

non-Windows

The logs are located in directories under `<base dir>/ragent/etc/logs.`

The default `<base dir>` is `/opt/imperva`

Windows

The logs are located in directories under `<base dir>\ragent\etc\logs.`

The default `<base dir>` is `C:\Program Files\Imperva`

For further information on changing the log level and logger directory for each monitor individually, see Show Counters on page 149.

Remote Agent Error Messages

If the remote Remote Agent fails to register to the SecureSphere gateway, the Remote Agent management console displays one the error messages listed in the table below.

Additional information is available in the Remote Agent Management Console log file (see Remote Agent Logs on page 153)

Errors and Possible Causes

Error	Possible Cause
"Unregistration/Registration failed! - failed to initialize HTTP client."	This message indicates a failure to initialize an HTTP client on the db host.
"Unregistration/Registration failed! - failed to send/ receive unregistration/registration data."	This message indicates that the remote agent failed to send or receive the registration data to the SecureSphere gateway. Check the connectivity between the DB host and the gateway listener as follows: `telnet` to the listener IP address on port 443 (unless changed through the gateway management console) and check if your listener accepts traffic on it (blank screen appear).
"Unregistration/Registration failed! - failed to send/ receive authorized unregistration/registration data."	This message indicates failure to send/receive authorized data.
"Unregistration/Registration failed! - bad password."	The password for the "Imperva" user on the gateway is incorrect. The default password is "secure". The user can change this password using the gateway's configuration management.

Errors and Possible Causes

Error	Possible Cause
"Unregistration/Registration failed! - missing registration/unregistration response data from the Gateway."	An empty response received from the gateway.

Maintenance Tasks

As a rule the Remote Agent does not require day-to-day maintenance. The Remote Agent management console allows you to control buffered files storage size and directory through the global settings menu. For more information, see Remote Agent Management Console on page 146.

Remote Agents in a Hypervisor (Virtualized) Environment

This section describes the issues arising when the Remote Agent is running in a hypervisor, for example, under VMware. The following issues are reviewed:

- If the MAC Address Changes on page 154

If the MAC Address Changes

You should configure the virtual NICs with fixed MAC addresses. However, if this is not feasible, then when the hypervisor changes the MAC address, you will have to re-register the Remote Agent.

To re-register a Remote Agent after its MAC address changes:

1. Unregister the Remote Agent.
2. Delete the Remote Agent from the workbench.
3. Re-register the Remote Agent.

Prerequisite Tests for non-Windows Agents

The tests listed below are performed as part of the pre-install script. The installation script will not install the Remote Agent if any of these tests fails.

The following section list the expected results of each of the tests for each platform.

Pre-Install Tests

Test ID	Test Name
1	OS compatibility
2	OS version
3	Platform compatibility
4	Kernel patch level
5	Kernel CPUs
6	Root volume
7	Disk space
8	Root permissions
9	Dependencies
10	Package instance
11	Executable instance
12	Driver instance
13	Temporary directory free space
14	Zone (Solaris)

It is possible to override these tests, that is, it is possible to ignore the results of a specific test. In this case, failure of the test will not prevent the Remote Agent's installation.

For example, one of these tests determines whether the Imperva Remote Agent is already running by searching for a process named `ragent`. If a process with that name, unrelated to Imperva, happens to be running, then the Remote Agent will not be installed unless that test is overridden.

You should address the issues raised by the test by correcting the problem, for example, by providing the necessary disk space. If necessary, contact Imperva support.

Solaris Pre-Install

Test Name	Test | Test Result
OS compatibility	SunOS
OS version	5.8/5.9/5.10
Minimum kernel patch level	Solaris 8 –108528-23 (issued on July 28,2003) Solaris 9 –112233-12 (issued on April 21, 2004) Solaris 10 –112233-12 (issued on April 21, 2004) **Note:** To determine the installed patch level, execute the following command: **`uname -a`**
Platform compatibility	sparc or x86_64
Root volume	Check that root volume exists. For example, if the specified root directory is **`/opt/imperva`**, check that **`/opt`** exists.
Disk space	Check that the sum of package file sizes is smaller than root volume directory free space. For example, if the specified root directory is **`/opt/imperva`**, check free space in **`/opt`**.
Root permissions	The user who installs and runs and runs the Remote Agent must belong to user group with root privileges.
Dependencies	not relevant
Executable instance	Check that there is no Remote Agent running process or existing installed package.
Driver instance	Check there is no Remote Agent module loaded in the kernel.
Temporary directory free space	Check that the **`/var/tmp`** directory free space is at least twice the size of the package (**`bsx`**) file.

Linux Pre-Install

Test Name	Test | Test Result
OS compatibility	'uname-s' == Linux
OS version	2.4/2.6
Kernel patch level	smp smp-hugemem smp-pae
Platform compatibility	x86_64 i386
Root volume	Check that root volume exists. For example, if specified root directory is **`/opt/Imperva`** check that **`/opt`** exists
Disk space	Check that the sum of package file sizes is smaller than root volume directory free space. For example, if specified root directory is **`/opt/imperva`** check free space in **`/opt`**
Root permissions	The user who installs and runs the Remote Agent must belong to user group with root privileges. For example, **`uid=1(other) gid=1(other)`** **`groups=1(other),0(root),2(bin),3(sys)`**
Dependencies	not relevant
Executable instance	Check that there is no Remote Agent running process or existing installed package.
Driver instance	Check that the following command returns an empty string. **`lsmod | grep krg`**
Temporary directory free space	not relevant

HP-UX Pre-Install

Test Name	Test | Test Result
OS compatibility	HP-UX
OS version	11.11/11.23/11.31
Kernel patch level	not relevant
Platform compatibility	PA-RISC/Itanium
Root volume	Check that root volume exists. For example, if the specified root directory is **`/opt/imperva`**, check that **`/opt`** exists.
Disk space	Check that the sum of package file sizes is smaller than root volume directory free space. For example, if the specified root directory is **`/opt/imperva`**, check the free space in **`/opt`**.
Root permissions	The user who installs and runs the Remote Agent must belong to user group with root privileges.
Dependencies	For non- kernel based agents the **`nettl`** executable must exist. From release 6.0.2.36 all HP-UX agents are kernel based.
Executable instance	Check that there is no Remote Agent running process or existing installed package.
Driver instance	Check that there is no Remote Agent driver instance running.
Temporary directory free space	Check that the **`/var/tmp`** directory free space is greater than package size.

AIX Pre-Install

Test Name	Test | Test Result
OS compatibility	AIX
OS version	5.2/5.3/6.1
Kernel patch level	The agent will not work with **bos.rte.libc** prior to 5.3.0.50, which is automatically installed by the 5300-05 kernel patch. To view the current value of **bos.rte.libc**, execute the following command: **lslpp -h bos.rte.libc**
Platform compatibility	powerpc32/64
Root volume	Check that root volume exists. For example, if the specified root directory is **/opt/Imperva**, check that **/opt** exists.
Disk space	Check that the sum of the package file sizes is smaller than root volume directory free space. For example, if the specified root directory is **/opt/imperva** check the free space in **/opt**
Root permissions	The user who installs and runs the Remote Agent must belong to user group with root privileges.
Dependencies	The **libpthread** shared library must exist.
Executable instance	Check that there is no Remote Agent running process or existing installed package.
Driver instance	Check that there is no Remote Agent driver instance running.
Temporary directory free space	Check that the **/var/tmp** directory free space is greater than package size.

Supported Interfaces for the Gateway Listener

In typical installations, the listener is configured with the gateway management IP address and uses the gateway management physical interface. The listener can be configured on other interfaces as well.

For example, an organizational security policy does not allow DB hosts to communicate with the gateway management IP / interface. The gateway management IP is on the OOB network and connects only to the management server. It is required to use another physical interface for the listener. To comply with the requirement, you can use the LAN interface of the gateway.

The table below provides detailed information about listener per physical interface combined with appliance mode.

Interfaces Supported in Listeners

GATEWAY MODE / INTERFACE	TCP	UDP
Bridge / data interfaces	✘	✘
Bridge / alternate management interface	✓	✓ – used for registration only. Agent UDP traffic must pass through the bridge.
Bridge / management interface	✓	✓ – used for registration only. Agent UDP traffic must pass through the bridge.
Sniffing / data interfaces	✓ – when data interface is not defined as sniffing.	✓ – must be defined as sniffing interface.
Sniffing / alternate management interface	✓ – when not defined as sniffing interface.	✓ – must be defined as sniffing interface or else used for registration only & sniffing interfaces listen to the Remote Agent UDP traffic.
Sniffing / management interface	✓	✓ – for registration only. Sniffing interfaces listen to the Remote Agent UDP traffic.

Terminology:

Data interface – non on-board interface, also known as a Quad card or Silicom card.

Alternate management interface – also known as LAN interface. A secondary on-board interface which is not used as the management interface.

Management interface – on board interface used for management.

✘ – not supported

✓ – supported

Advanced Agent Configuration

This section includes the following information:

- UDP Tunnel Mode on page 161
- UDP Listener Configuration on page 162
- Working with a NATed Listener on page 163
- Working with Multiple Oracle Instances on page 165
- Monitoring Solaris Zones Using Remote Agents on page 166
- Monitoring MySQL Traffic on page 167
- RWorking with DAC (Dedicated Administrator Connection) on page 167

UDP Tunnel Mode

UDP mode can be used when the Remote Agent and gateway listener cannot establish direct communication. In UDP mode, the Remote Agent opens a unidirectional tunnel to a remote location behind the gateway (usually remote router). The gateway topology could be either bridge or sniffing. SecureSphere gateway analyzes this traffic like any other traffic and drops it on the interfaces.

Note:
- Only the data channel can use UDP.
- If the listener IP address is NATed, see Working with a NATed Listener on page 163.
- Large Segment Offload traffic (LSO) is not supported in UDP mode.

To Configure UDP Tunnel Mode:

1. Add a UDP listener on the gateway.
2. Configure the Remote Agent to use UDP mode. See Registering the Remote Agent to the Gateway on page 147.

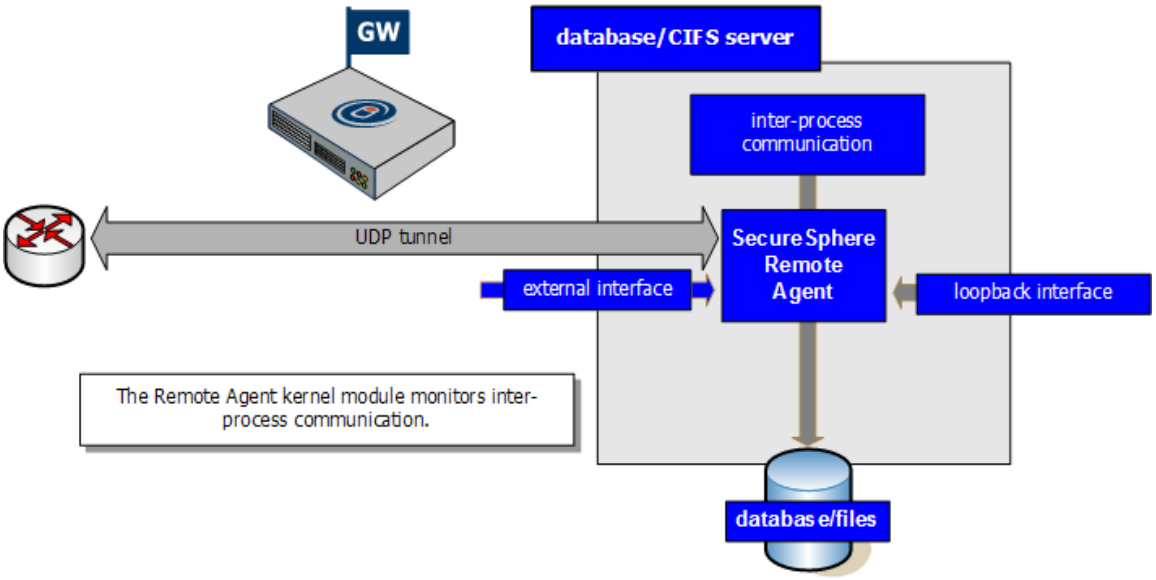


Figure 40 Typical UDP Scenario

High Availability in UDP Mode

When using UDP, you can achieve high availability using VRRP. If your topology uses gateway High Availability using VRRP, (bridge STP or Imperva HA bridge), complete the Remote Agent registration process with both gateways. This will ensure that after failover, agent traffic is processed by the backup gateway if and when it takes over.

For more information, see Registering the Remote Agent to the Gateway on page 147.

UDP Listener Configuration

When a Remote Agent is configured on a system, it sends traffic over UDP to the gateway. Since that UDP port is not bound to any process on the gateway, it sends out an ICMP destination unreachable message for each packet it receives. Potentially this could create a packet storm if the Remote Agent traffic is heavy enough.

To make the gateway drop all ICMP destination unreachable packets:

1. Using a text editor, open the file **`/opt/SecureSphere/etc/impctl/lib/portguard.sh`**
2. In the section **`portguard_start()`**, look for the following:

```
        ##########################
        # IPTABLES Configuration
        ##########################

    210 if [ "${allowed_ports}" ]; then
    211                 if [ "${allowed_ip_addresses}" ]; then
    212                         for addr in ${allowed_ip_addresses}; do
    213                                 ${_portguard_iptables_bin} --append
${chain}                        \
    214                                                         --source
${addr}                         \
    215                                                         --protocol
tcp                             \
    216                                                         -m
multiport                                 \
    217                                                         --dports
${allowed_ports//[[:space:]]/,} \
    218                                                         --jump ACCEPT > /dev/
null 2>&1
    219                         done
    220                 fi
    221                 ${_portguard_iptables_bin} --append
${chain}                        \
    222                                         --protocol
tcp                             \
    223                                         -m
multiport                                 \
    224                                         --dports     ${allowed_ports//
[[:space:]]/,} \
    225                                         --jump       DROP > /dev/null 2>&1
    226 /sbin/iptables -A OUTPUT -o eth0 -p icmp --icmp-type 3 -j DROP
    227         fi
```

3. Apply the following IP tables rule for each interface (the example below is for eth0) by adding the line below to the file. This line is shown in the code above.

```
iptables -A OUTPUT -o eth0 -p icmp --icmp-type 3 -j DROP
```

4. Save the file.
5. Restart **portguard** using the following command:

```
impctl portguard restart
```

6. You need to define a NIC as sniffing device. The gateway needs to be in sniffing. If the gateway is in bridge mode you need to pass the UDP traffic through the bridge.

Working with a NATed Listener

Depending on the topology, the configured gateway listener IP address is sometimes NATed by a firewall (or other device) situated between the database server and the gateway. When working with a NATed listener or when a firewall is present, some additional configuration is required.



Note: If the gateway is NATed, then the agent's **bootstrap.xml** and **ctrl.xml** files are updated with the internal IP address.

Communication to and from the listener NAT must be allowed through the firewall. This includes the listener IP address, the listener high port and the listener registration port (usually 443).

Working with a NATed Listener in Non-Windows Environments

After registering the Remote Agent with the gateway, the gateway configures the Remote Agent configuration files **<base dir>/ragent/etc/bootstrap.xml** and **<base dir>/ragent/etc/ctrl.xml** with the IP address of the listener. If NAT is used for the listener IP address, this information must be edited with the NAT IP address as follows.

1. Successfully register the Remote Agent with the gateway (see Registering the Remote Agent to the Gateway on page 147).
2. Backup (copy) the Remote Agent configuration files **<base dir>/ragent/etc/bootstrap.xml** and **<base dir>/ragent/etc/ctrl.xml**.
3. Edit the Remote Agent configuration files **<base dir>/ragent/etc/bootstrap.xml** and locate the tag **<data-tunnel>**. Below this tag search for **<gw-ip>**, which includes the listener real IP address.
4. Replace the IP address with the NAT IP address.
5. Make the same change in the **<base dir>/ragent/etc/ctrl.xml** file.

EXAMPLE:

Given the following information:

- The real listener IP address is 1.2.3.4
- The listener port is 5678
- The listener NAT IP address is 11.12.13.14

The configuration files **<base dir>/ragent/etc/ragent.xml** and **ctrl.xml** will at first look like this:

```
<data-tunnel>
    <gw-ip>1.2.3.4</gw-ip>
    <gw-port>5678</gw-port>
    <gw-ssl>true</gw-ssl>
    <protocol>TCP</protocol>
    <registered>true</registered>
   </data-tunnel>
```

After the change, the configuration files will look like this (the changed portion is shown here in bold):

```
<data-tunnel>
    <gw-ip>11.12.13.14</gw-ip>
    <gw-port>5678</gw-port>
    <gw-ssl>true</gw-ssl>
    <protocol>TCP</protocol>
    <registered>true</registered>
   </data-tunnel>
```

Working with a NATed Listener in Windows Environments

After registering the Remote Agent with the gateway, the gateway configures the Remote Agent configuration files **<base dir>\RemoteAgent\bootstrap.xml** and **<base dir>\RemoteAgent\ctrl.xml** with the IP address of the listener. If NAT is used for the listener IP address, this information must be edited with the NAT IP address as follows.

1. Successfully register the Remote Agent with the gateway (see Registering the Remote Agent to the Gateway on page 147).
2. Backup (copy) the Remote Agent configuration files **<base dir>\RemoteAgent\bootsrap.xml** and **<base dir>\RemoteAgent\ctrl.xml**.
3. Edit the Remote Agent configuration file **<base dir>\RemoteAgent\bootstrap.xml** and locate the tag **<data-tunnel>**. Below this tag search for **<gw-ip>**, which includes the listener real IP address.
4. Replace the IP address with the NAT IP address.
5. Make the same change in the **ctrl.xml** file.

EXAMPLE:

Given the following information:

- The real listener IP address is 1.2.3.4
- The listener port is 5678
- The listener NAT IP address is 11.12.13.14

The configuration files **<base dir>\RemoteAgent\bootsrap.xml** and **<base dir>\RemoteAgent\ctrl.xml** will at first look like this:

```
<data-tunnel>
    <gw-ip>1.2.3.4</gw-ip>
    <gw-port>5678</gw-port>
    <gw-ssl>true</gw-ssl>
    <protocol>TCP</protocol>
   </data-tunnel>
```

After the change, the configuration files will look like this (the changed portion is shown here in bold):

```
<data-tunnel>
    <gw-ip>11.12.13.14</gw-ip>
    <gw-port>5678</gw-port>
    <gw-ssl>true</gw-ssl>
    <protocol>TCP</protocol>
   </data-tunnel>
```

Working with Multiple Oracle Instances



Note: The Remote Agent automatically discovers all the Oracle servers on a DB host and creates the required data interaces. This section is relevant only if for some reason you want to configure a data interace.

A DB host configuration may include multiple Oracle servers installed. In such cases there will be multiple BEQ/IPC adapters, each with a unique path to the executable. You might want to only monitor specific adapters.

As an example, consider BEQ. For each of the databases installed there will be a BEQ adapter configured with each PROGRAM parameter pointing to a different full path to the Oracle executable. **$ORACLE_HOME** path is specific for each installation, but the executable name is the same - **Oracle**.



Note: When you configure the Remote Agent to add a local Oracle monitor, you must enter the monitor service name. Service name in the Remote Agent terminology is the BEQ PROGRAM parameter value, or if you configure IPC, its KEY parameter value. The Remote Agent matches service name as a suffix.

If you would like the Remote Agent to monitor all BEQ processes on the DB host, specify **Oracle** as the service name, which is also the value suggested by the Remote Agent Management Console. However if you want to monitor only a specific BEQ adapter, then specify the full path or the suffix that makes it unique.

The same concept applies to IPC if its names are unique.

In some cases the **tnsnames.ora** file may not include the above information. This does not mean that no Bequeath adapter is configured. There is always a default Bequeath adapter configured pointing to the “oracle” executable. To find more details about the relevant instance you can examine the **listeners.ora** file under the **$ORACLE_HOME/network/admin/** directory.

EXAMPLE:

Below is a typical **tnsnames.ora** configuration file with TCP, BEQ and IPC configuration. The parameters relevant to the Remote Agent configuration are in bold.

```
ORCL =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP)(HOST = 127.0.0.1)(PORT = 1521))
    )
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = orcl)
    )
  )

IPC =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = IPC)(KEY = orcl))
    )
    (CONNECT_DATA =
      (SERVICE_NAME = orcl)
    )
  )

ORA920BEQ =
   (DESCRIPTION =
    (ADDRESS_LIST =
     (ADDRESS = (PROTOCOL = BEQ)(PROGRAM=/export/home/Oracle/OraHome1/bin/
Oracle")
   (argv0=beq920)
      (args='(DESCRIPTION=(LOCAL=YES)(ADDRESS=(PROTOCOL=BEQ)))')
      (envs='Oracle_HOME=/export/home/Oracle/OraHome1/,ORACLE_SID=orcl')
      )
     )
)
```

Monitoring Solaris Zones Using Remote Agents

In the Solaris Zones architecture, all traffic passes through the global zone. When installing Remote Agent in a Solaris zones configuration, it must be installed in the global zone only. From the global zone, the agent monitors access to databases in all zones.

When monitoring TCP traffic the zones are differentiated using the IP address. To monitor traffic from the specific zone, configure the correct IP address in the TCP data interface. For more information, see the ***SecureSphere User Guide***.

When monitoring Oracle IPC or Oracle BEQ, the zone name should be added as a prefix to the Server Path parameter using the ':' separator.

For example: `zone1:/opt/oracle/product`.

Global zone should not be added as prefix, regardless if zones are enabled or not on the machine.

For discovered interfaces the relevant zone is reported as the property “Zone” (see Monitoring Solaris Zones Using Remote Agents on page 166).

Monitoring MySQL Traffic

By default, the MySQL Unix clients connect to the MySQL database over a Unix domain socket. In order for the Remote Agent to monitor this type of connection, this traffic must be redirected to the loopback interface.

To redirect MySQL traffic to the loopback interface:

1. Open the MySQL configuration file with a text editor.
   The default MySQL configuration file is `/etc/my.cnf`
2. In the `[client]` section, add the following line:

```
protocol=TCP
```

3. Save the file.
4. Restart the MySQL server.

RWorking with DAC (Dedicated Administrator Connection)

When working with DAC, the MSSQL service listens locally on an additional port, by default locally only. Usually the service uses the port following the default MSSQL port, that is, 1433. If the port already in use, it will use a different port.



Note: To determine the additional local port on which the sql service is listening, use the following command:

```
netstat -anb
```

To support monitoring of DAC traffic:

1. Configure the DAC service port in the SecureSphere GUI under the service ports definitions (**Setup** > **Sites** > **Service** > **Definitions** tab > **Ports**.
2. Configure the agent to monitor the loopback interface.

Command Line Scripting Language



Note: This section is aimed at advanced users which know how to use Remote Agent and scripting.

The Imperva Remote Agent provides a scripting language to configure the Remote Agent. This capability allows you to install and register agents using software distribution tools in large environments.

The Remote Agent command line accepts input from a file with script commands to automatically configure the Remote Agent.

This section includes the following information:

- Conventions for Command Line Scripting on page 168
- Syntax for Command Line Scripting on page 169

Conventions for Command Line Scripting

- You can see all the options using the tab key.
- Options are equivalent to the Remote Agent Management Console menus.
- <TAB> lists all options and complete the command when the command prefix is typed.
- After completing the first word in the command, <TAB> will again show you all possible options.
- Save is perform automatically when completing a command, in contrast to the Remote Agent management console mode (mode menu).
- Enter **exit** to exit the shell.

To start the command line in scripting shell, do one of the following:

non-Windows:

Execute the following command:

```
.<base dir>/ragent/bin/racli shell
```

The default **<base dir>** is **/opt/imperva**

Windows:

- Execute the following command:

```
<base dir>\RemoteAgent\StartCli.bat
```

The default **<base dir>** is **C:\Program Files\Imperva**

- Choose option 3 Shell Mode.
- Execute the following command:

```
RemoteAgentCli.exe -mode shell -dcfg  "C:\Program Files\Imperva\RemoteAgent" -
dlog "C:\Program Files\Imperva\RemoteAgent\logs" -dtarget "C:\Program
Files\Imperva\RemoteAgent"
```

Syntax for Command Line Scripting

non-Windows

Command line shell options are equivalent to the Remote Agent management console elements. This section discusses example configuration only. It does not list full menu of the available operations. Below you will find examples. See Remote Agent Management Console on page 146 for details on the meanings of these elements.

Pressing **<TAB>** at the **dbagent>** shell prompt will display all available options:

```
dbagent>
  registration: Manage Database Agent Registration
  actions: Perform Actions (Start/Stop/Restart)
  trouble-shooting: Trouble Shooting
  shell-script: Read shell script from an input file.
```

Remember to register and start the Remote Agent if needed.

If **my file name and location** is **/tmp/myconfigurationscript,** then the command is:

```
dbagent> shell-script directory=<The script file directory> file=<The script
file name>
dbagent>  shell-script directory=/tmp file=myconfigscript
```

To run it automatically from a script, use the following command:

```
<base dir>/ragent/bin/cli -mode <shell/menu/script> -dcfg <cfg-dir-path>
   -dlog <log-dir-path> -dtarget <target-dir-path> <params>
```

Option	Description
-dcfg	The path to the **cli.xml** file. When the default installation is used, the path is **/opt/imperva/ragent/etc**
-dlog	The log directory. When the default installation is used, the log directory is **/opt/imperva/ragent/etc/logs**
-dtarget	The target directory for the Remote Agent configuration file **ragent.xml** When the default installation is used, the target directory is **/opt/imperva/ragent/etc**

```
.<base dir>/ragent/bin/cli -dcfg /opt/imperva/ragent/etc
    -dlog /opt/imperva/ragent/etc/logs
    -dtarget /opt/imperva/ragent/etc  shell-script directory=/tmp
    file=myconfigscript
```

Windows

Command line shell options are equivalent to the Remote Agent management console elements. This section discusses an example configuration only. It does not list full menu of the available operations. See Remote Agent Management Console on page 146 for details on the meanings of these elements.

Pressing **<TAB>** at the **>** shell prompt will display all available options:

```
>
  registration: Manage Database Agent Registration
  actions: Perform Actions (Start/Stop/Restart)
  trouble-shooting: Trouble Shooting
  shell-script: Read shell script from an input file
```

Remember to register and start the Remote Agent if needed.

If **my file name and location** is **\temp\myconfigurationscript**, then the command is:

```
> shell-script directory=<The script file directory>
   file=<The script file name>
> shell-script directory=\temp file=myconfigscript
```



Note: Use the **ListPcapDevices.exe** tool, available from the Imperva FTP server under the agent installation directory, to get the names of the network interfaces.

If you would like to run it automatically from a script, use the following command:

```
<base dir>\RemoteAgentCli.exe -mode <shell | menu | script>
-dcfg <cfg-dir-path> -dlog <log-dir-path> -dtarget <target-dir-path> <params>
```

Option	Description
-dcfg	The path to the **cli.xml** file. When the default installation is used, the path is **C:\Program Files\Imperva\RemoteAgent**
-dlog	The log directory. When the default installation is used, the log directory is **C:\Program Files\Imperva\RemoteAgent\logs**
-dtarget	The target directory for the Remote Agent configuration file **bootsrap.xml** When the default installation is used, the target directory is **C:\Program Files\Imperva\RemoteAgent**

For example, if you have a script (see previous example) to run under the command line, execute:

```
<base dir>\RemoteAgentCli.exe -dcfg "C:\Program Files\Imperva\RemoteAgent"
-dlog "C:\Program Files\Imperva\RemoteAgent\logs"
-dtarget "C:\Program Files\Imperva\RemoteAgent" shell-script directory=\temp
file=myconfigscript
```



Note: The path used must be enclosed in double quotes.

CHAPTER 6

Installing SecureSphere Agent for DB2 z/OS

This chapter describes how to install and configure SecureSphere Agent for DB2 z/OS and provides the following information:

Installing SecureSphere Agent for DB2 z/OS - Version 2.1 on page 173
Installing SecureSphere Agent for DB2 z/OS - Version 1.3 on page 191



Note: For information on configuring SecureSphere Agent for DB2 z/OS in SecureSphere, see the "Remote Agents" chapter in the ***SecureSphere User Guide***.

Installing SecureSphere Agent for DB2 z/OS - Version 2.1

This section contains the following information:

Upgrading from Version 1.3 to Version 2.1 on page 173
Configuring SecureSphere Agent for DB2 z/OS Tasks on page 173
Before Installing and Configuring SecureSphere Agent for DB2 z/OS on page 174
Downloading and Installing SecureSphere Agent for DB2 z/OS on page 177
Configuring SecureSphere Agent for DB2 z/OS (on z/OS) on page 180
Starting, Managing, and Stopping SecureSphere Agent for DB2 z/OS on page 189

Upgrading from Version 1.3 to Version 2.1

SecureSphere Agent for DB2 z/OS version 1.3 and version 2.1 cannot be running at the same time on the DB2 server.

To upgrade from SecureSphere Agent for DB2 z/OS version 1.3 to version 2.1:

1. Stop the previous version using the following command:

```
/P process_name
```

For example,

```
/P NSUPROC
```

2. In the SecureSphere GUI, delete the SecureSphere Agent for DB2 z/OS that you just stopped.
3. Install SecureSphere Agent for DB2 z/OS version 2.1.
4. Install the latest maintenance.



Note:

- Do not run the version 1.3 and version 2.1 SecureSphere Agent for DB2 z/OS at the same time.
- If you want to restore a previous SecureSphere Agent for DB2 z/OS, follow the above procedure, that is, stop the agent, delete it from the GUI and install the other version and its maintenance.

Configuring SecureSphere Agent for DB2 z/OS Tasks

The SecureSphere administrator must perform the tasks described below.

	Task Overview	For more information, see...
	Make the necessary preparations for installing SecureSphere Agent for DB2 z/OS.	Before Installing and Configuring SecureSphere Agent for DB2 z/OS on page 174
	Download and install the SecureSphere Agent for DB2 z/OS.	Downloading and Installing SecureSphere Agent for DB2 z/OS on page 177
	Configure the SecureSphere Agent for DB2 z/OS license.	Specifying the License Key on page 181

	Task Overview	For more information, see...
	Using `impcfg`, configure the data and configuration channels on which SecureSphere Agent for DB2 z/OS communicate with the SecureSphere gateway. **Note:** A Remote Agent listener and a SecureSphere Agent for DB2 z/OS listener cannot be defined on the same port.	Adding a SecureSphere Agent for DB2 z/OS Listener on page 79

Before Installing and Configuring SecureSphere Agent for DB2 z/OS

There are a number of items you should verify and understand before beginning to install and configure SecureSphere agent for z/OS. This includes:

- Information You Must Have Before You Begin on page 174
- Terminology Used In This Guide on page 174
- Roles and Assignments for the Installation and Configuration on page 175
- Mainframe Software Requirements on page 176
- Security Requirements on page 176
- TCP/IP Requirements on page 177
- Optimizing Performance on page 177
- Supported Facilities on page 177

Information You Must Have Before You Begin

Verify that you have the following items:

Item	Additional Information
Credentials to access the Imperva FTP site	You use the credentials to access the FTP site and to download and install SecureSphere Agent for DB2 z/OS files.
License key for the SecureSphere Agent for z/OS	You must specify the license key when you install the SecureSphere Agent for z/OS on the z/OS host.

Terminology Used In This Guide

The product includes the following components.

- A component referred to as SecureSphere Agent for z/OS, that runs as a started task and gathers data about the DB2 subsystems being audited.
- A component referred to as the SecureSphere Gateway, that receives all the information gathered by SecureSphere Agent for z/OS.
- A component referred to as SecureSphere Management Server, that provides the collection rules to SecureSphere Agent for z/OS.

Roles and Assignments for the Installation and Configuration

Depending on the size and complexity of your IT organization, several people might contribute to the SecureSphere Agent for DB2 z/OS installation and configuration process. In most cases, these are the roles and their specific skills or knowledge.

- DB2 DBA or System Administrator
- Network Administrator
- Security Administrator
- System Programmer

The matrix shows:

- In order, the tasks that you perform during the installation and configuration (The tasks in the table are covered in the topics that follow.)
- In most cases, who in the organization will be involved in completing those tasks

Location in the Process	Installation and Configuration Task	Role			
		DB2 DBA	Network Administrator	Security Administrator	System Programmer
Before you install SecureSphere Agent for DB2 z/OS	Authorize any required TCP/IP connections and provide information that the System Programmer uses during product customization.		X		
	Define mainframe TCP/IP authority.			X	
Downloading and installing SecureSphere Agent for DB2 z/OS	Install the product by downloading a job that allocates the data sets and then copies the product libraries to z/OS.				X
Configuring SecureSphere Agent for DB2 z/OS	Specify the license key and product libraries on z/OS.				X
	Application Program Facility (APF) authorize the LOAD library and make the authorization permanent following an IPL. (You do not have to IPL the system to install the product.)				X
	Specify the customization parameters specific to DB2 (such as the load libraries for the versions of DB2).	X			X
	Specify the customization parameters specific to TCP/IP (such as the port numbers for the data receiver and plan provider). **Note:** For more information, see Adding a SecureSphere Agent for DB2 z/OS Listener on page 79.		X		X

Location in the Process	Installation and Configuration Task	Role			
		DB2 DBA	Network Administrator	Security Administrator	System Programmer
Completing the configuration for the started task	Bind the DB2 packages for the product.	X			
	Authorize the started task for the product so that it can access the required resources.			X	
	Grant DB2 privileges to the user ID for the started task so that it can access the DB2 Catalog for any DB2 instance being audited.	X		X	
	Initialize and secure the rules data sets for the product so that it can only be modified by the started task.			X	X
	Specify a priority for the started task in Workload Manager (WLM).				X
	Modify the started task procedure and copy the procedure to the SYSPROC library,				X
Starting, managing, and stopping SecureSphere Agent for DB2 z/OS	Start the started task.				X

Mainframe Software Requirements

Before unloading and installing SecureSphere Agent for z/OS, verify that you have the following software installed and operational on your z/OS system.

- IBM z/OS version 1.8 or later (64 bit mode required)
- DB2 for z/OS version 8, 9 or 10
- IBM TCP/IP version 3.1 or later

Security Requirements

The table lists the security requirements for SecureSphere Agent for z/OS.

Element	Security Requirement
DB2	You must authorize the started task-user ID so that it can access the DB2 Catalog for any DB2 instance being audited.
Rules data sets	You must protect the rules data sets for SecureSphere Agent for z/OS so that it can only be modified by the started task. You will specify the rules data sets using the Local Rules Dataset Name customizable parameter when you configure SecureSphere Agent for DB2 z/OS.

Element	Security Requirement
Started task	For the product to run successfully, you must provide SecureSphere Agent for z/OS with adequate authority to operating system and database resources. Using your security administration product (such as RACF), you should establish application profiles for the started task. For example, the started task for the product uses TCP to communicate with the Imperva. If you are using RACF, the started tasks for the product must have an OMVS segment defined in RACF.

TCP/IP Requirements

You must have TCP/IP network connections between the LPAR where auditing is performed and the SecureSphere Gateway and SecureSphere Management Server.

Before installing the product, you will need the:

- TCPIP.DATA data set name
- TCP/IP port numbers for the data receiver and plan provider (for more information, see Adding a SecureSphere Agent for DB2 z/OS Listener on page 79)
- Host name for the data receiver and plan provider
- You will also need to define mainframe TCP/IP authority.

Optimizing Performance

The product is architected for optimal performance so that auditing activities never impact normal business transaction processing. Key performance features include:

- When available, use of zIIP processors
- No reliance on slow, resource-intensive database trace utilities
- Off loads audit data from mainframe so that analysis, reporting, and data storage expenses are not incurred on the mainframe

Supported Facilities

The product supports the following local attach facilities for DB2 on z/OS:

- Call Attach (CAF)
- Resource Recover Services (RRSAF)
- CICS
- TSO
- IMS

The product also supports DRDA for distributed connections.

Downloading and Installing SecureSphere Agent for DB2 z/OS

This topic contains information about how to download and install SecureSphere Agent for DB2 z/OS. It includes:

- Downloading and Installing the Product on page 178
- APF Authorizing the LOAD Library on page 179
- Creating the ADMIN Library on page 179
- Including the Product Libraries in Your Disaster Recovery Plan on page 180

Downloading and Installing the Product

The section describes the prerequisites and procedures required for downloading and installing SecureSphere Agent for DB2 z/OS and includes:

Prerequisite for Downloading and Installing the Product or Cumulative Maintenance on page 178

Procedure for Downloading and Installing the Product on page 178

Procedure for Downloading and Installing the Cumulative Maintenance on page 178

Prerequisite for Downloading and Installing the Product or Cumulative Maintenance

To unterse the files, you must have installed TRSMAIN V4 or AMATERSE.



Note: AMATERSE is an enhanced replacement for TRSMAIN and it is strongly recommended that you upgrade from TRSMAIN V4 to AMATERSE.

For information about installing or upgrading to AMATERSE, see http://techsupport.services.ibm.com/390/trsmain.html.

Procedure for Downloading and Installing the Product

This section contains the procedures you follow to download and install the product for the first time or upgrade the product to a new version or release.



Note: When you download and install the product, also be sure to download and apply any cumulative maintenance included in the FTP directory. Skipping this step may cause the product to behave incorrectly.

If you have already installed the product and only need to install cumulative maintenance, see Procedure for Downloading and Installing the Cumulative Maintenance on page 178.

To download and install the product files:

1. From the FTP site, download the file **`readme.txt`**. This file describes the datasets contained within the directory. Additionally, it may contain special instructions regarding the download process that are not included in this document.
2. If JCL is needed to unterse the install file, from the FTP site, download the file **`unpack.jcl`**, a JCL file that contains sample JCL using TRSMAIN or AMATERSE.
3. Transfer the tersed product file to your mainframe system. The install process is started by untersing a single dataset. This dataset is described in the readme.txt file. This dataset may be downloaded directly to your mainframe system if the mainframe system has an internet connection, or it may be downloaded to an interim system first and then uploaded to the mainframe.
4. Follow the instructions in the RECVBASE member of the resulting untersed file. When submitted, this job will execute the TSO RECEIVE command to create the product datasets from the remaining members contained within the untersed dataset.

Procedure for Downloading and Installing the Cumulative Maintenance

This section contains the procedures you follow to download and install the cumulative maintenance.

To download and install the maintenance files for an existing installation:

1. From the FTP site, download the file **`readme.txt`**. This file describes the datasets contained within the directory. Additionally, it may contain special instructions regarding the download process that are not included in this document.
2. If JCL is needed to unterse the cumulative maintenance file, from the FTP site, download the file **`unpack.jcl`**, a JCL file that contains sample JCL using TRSMAIN or AMATERSE.
3. Transfer the tersed cumulative maintenance file to your mainframe system. The maintenance process is started by untersing a single dataset. This dataset is described in the readme.txt file. This dataset may be

downloaded directly to your mainframe system if the mainframe system has an internet connection, or it may be downloaded to an interim system first and then uploaded to the mainframe.

4. Follow the instructions in the RECVFIXS member of the resulting untersed file. When submitted, this job will execute the TSO RECEIVE command and update your product libraries from the remaining members contained within the untersed dataset.

APF Authorizing the LOAD Library

The product uses dataspaces, cross memory services, and other functions that require APF authorization. These are common and necessary requirements of system level software. The library that contains SecureSphere Agent for z/OS LOAD modules (*?neonhlq*.LOAD) must be APF authorized.

You must also ensure that the authorization is permanent to prevent losing authorization at your next IPL.

To APF authorize the LOAD library, your system programmer must issue an APF command. The table shows examples of the commands.

Status of the Data Set for the LOAD Library	Example Command
Managed by the IBM System Management Service (SMS)	SETPROG APF,ADD,DSNAME=*?neonhlq*.LOAD,SMS
Not managed by SMS	SETPROG APF,ADD,DSNAME=*?neonhlq*.LOAD,VOLUME=*volume*

Once the LOAD library has been APF authorized, updates or changes made to the configuration using the Product Customization Facility must be done by someone with authority to update an APF authorized library. (This person is typically not a DBA.)

Creating the ADMIN Library

The product uses an administration (ADMIN) library to manage and maintain product keys and the associated product libraries. You must allocate and catalog this ADMIN library.



Note: You must create the ADMIN library only if you are installing the product for the first time.

Follow this process.

1. Locate the ALLOCATE member in the *?neonhlq*.CNTL data set.
2. Modify the sample JCL using the instructions included in the member.
3. Submit the job to allocate the library.

   Result: The job allocates a data set with the format shown in the following table:

Item	Value
Data set format	Partitioned data set (PDS)
Record format	Fixed block (FB), 80-character logical records LRECL=80, RECFM=FB,*blksize* Where *blksize* is your site standard block size.
Allocated space	Two tracks and 10 directory blocks

Including the Product Libraries in Your Disaster Recovery Plan

The product includes the data sets listed in the table below. These resources should also be included in your backup and disaster recovery plan.

Data Set Name	Description
?neonhlq.ADMIN	This library contains product keys.
?neonhlq.CNTL	This library contains the control members for SecureSphere Agent for z/OS, including sample JCL.
?neonhlq.DBRMLIB	This library contains the DB2 definitions for SecureSphere Agent for z/OS.
?neonhlq.EXEC	This library contains the REXX executables needed to configure SecureSphere Agent for z/OS.
?neonhlq.LOAD	This library contains the executable LOAD modules needed to execute SecureSphere Agent for z/OS.
?neonhlq.MESSAGES	This library contains descriptions for product messages.
?neonhlq.MLIB	This library contains messages issued by the ISPF interface.
?neonhlq.MSG	This library contains the message modules used by SecureSphere Agent for z/OS.
?neonhlq.PLIB	This library contains ISPF panels used by SecureSphere Agent for z/OS.

Configuring SecureSphere Agent for DB2 z/OS (on z/OS)

This topic contains information about using the Product Customization Facility to configure SecureSphere Agent for DB2 z/OS and includes:

- Accessing the Product Customization Facility on page 180
- Specifying the License Key on page 181
- Specifying the Product Libraries on page 182
- Specifying the Customizable Parameters on page 182
- Detailed Information About the Customization Parameters on page 184
- Completing the Configuration on page 187
- Binding Packages for the Product on page 206
- Granting DB2 Privileges on page 187
- Initializing and Securing the Rules Data Set on page 188

Accessing the Product Customization Facility

Follow this process to access the Product Customization Facility. You must access the Tomium Product Customization Facility if you are:

- installing the product for the first time
- upgrading to a new version or release of the product

1. At the TSO prompt (option 6), specify the following command.

   EX '*?neonhlq*.EXEC(NEONCNTL)' '*?neonhlq*'

   Where *?neonhlq* is the high-level qualifier for SecureSphere Agent for z/OS LOAD library that you specified when you installed SecureSphere Agent for z/OS.

Result: The product displays the Product Customization Facility menu.

```
                  NEON Product Customization          Row n to n of n
Command ===> _____________________________________________ Scroll ===> CSR

   Product load library. . . ?neonhlq.LOAD

Type S to select a product for customization, B to BROWSE the $README member

   Product Name / Description                                  Version
 _ License Management                                          nn.nn.nn
```

Specifying the License Key

You received a license key for SecureSphere Agent for DB2 z/OS when you purchased SecureSphere Agent for z/OS. This license key is required to run SecureSphere Agent for z/OS and protects the software from unauthorized use. You must specify the license key if you are:

- installing the product for the first time
- adding new keys or removing old keys

If the proper product keys are not present SecureSphere Agent for z/OS will fail.Follow this process to specify the license key.

1. Type **S** next to License Management.
2. Press Enter.
3. On the NEON Enteprise Software Product Key Update panel, specify:
4. **Y** in the Manage Product Keys field
5. **Y** in the Manage Product Libraries field
6. Press Enter.

   Result: The panel redisplays with these values:

Field	Description
Product Name	Name of the family of products for this key
CPU Id	Processor id for which this key is valid
Expires	Expiration date for this key
Features	All feature codes in the key

7. Type **End** on the command line and press Enter or press the appropriate function key.

   Result: The Product Customization Facility displays the next Enterprise Software Product Key Update panel in the series.

Specifying the Product Libraries

You must specify the product libraries if you are:

- installing the product for the first time
- upgrading to a new version or release of the product

This step ensures that there is a locator module in SecureSphere Agent for z/OS LOAD library. (The locator module indicates where the license keys are stored.) Without this module SecureSphere Agent for z/OS will not be able to perform product key validation and SecureSphere Agent for z/OS will fail. Follow this procedure to specify SecureSphere Agent for z/OS libraries.

1. On the NEON Enteprise Software Product Key Update panel, specify:
   1.1 The fully qualified data set name of the ADMIN library that you allocated in the NEON Administration Library field (Do not specify quotes around the name.)
   1.2 Your license key in the Product Key field
2. Press Enter.
3. Verify that the Status column displays Locator correct.
4. Type **End** on the command line and press Enter or press the appropriate function key.

   Result: The Product Customization Facility redisplays the Product Customization Facility menu.

   The table describes the remaining fields on the panel.

Field	Description
LC	Use this field to update (U) or delete (D) libraries.
Product Library	Lists the NEON Enteprise Software product LOAD libraries contained in the ADMIN data set library. Each library contains a locator module, which identifies the location of the ADMIN library.
Status	Describes the status of the locator module

Specifying the Customizable Parameters

You must specify the customizable parameters if you are:

- installing the product for the first time
- upgrading to a new version or release of the product

If you are upgrading and you want to use the existing values for the customization parameters, you can save the existing values by accessing the panel and pressing END to save and exit the panel.



Note: You must perform this step if you are installing or upgrading the product. Saving and exiting the panel activates the NSUUOPT module that contains the customizable parameters. If you are upgrading, saving and exiting the panel upgrades the module so that it is at the same version and release level as the product.

Follow this procedure.

1. On the Product Customization Facility menu, type **S** next to SecureSphere Agent for DB2 z/OS and press Enter.

   Result: The Product Customization Facility displays the SecureSphere Agent for DB2 z/OS **Customization Options** panel.

```
-------- NEON Database Activity Monitor Customization Options Vnn.nn.nn ------
Command ===>
                                                                More:    - +
     Product Load Library . . ?neonhlq.LOAD
     Options Module Name. . . NSUUOPT
     Note: Parameters Initialized to NEON Recommended Values

 SecureSphere Agent for z/OS Database Activity Monitor Message Log Parameters:
  Message Data Set Name. . . . . --------
  Message Language . . . . . ENU                    ENU
  Message Set. . . . . NSU01                         NUS01
  Sysout (NSUPRINT) Message Level  2                 1 - 3  ( 3 = Verbose )

 SQL Related Parameters:
  Package Collection ID  . . . . . NSUD210          DB2 Collection Name
  SQL Retry Delay. . . . . 1                        0 - 9999 Seconds
  Number of SQL Retries. . . . . 5                  0 - 9999 Attempts
  -DISPLAY LOCKS for -913 Retries. N                N - Never
                                                    R - For Every retry
                                                    F - Only for Failure

 Communication Parameters:
  Inactivity Disconnect Timeout  . 300               1 to 6000 Seconds
  Data Receiver Port Number. . . .                   1 to 65535
  Data Receiver Host Name. . . . .
  Plan Provider Port Number. . . .                   1 to 65535
  Plan Provider Host Name. . . . .


 General Operating Options:
  Max Dataspace Size . . . . . 100                  1 to 2047 Megabytes
  Local Rules Dataset Name . . . .

 DB2 Environment Information:
  DB2 Version 8 Load Library . . .
  DB2 Version 9 Load Library . . .
  DB2 Version 10 Load Library . . .
  Resolve Group Attach Name. . . . Y                 Y-Yes  N-No
  DB2 Subsystems Selected for Audit


Press ENTER to update END to save and exit
      CANCEL to exit ignoring any changes made since the last update
```

Figure 41 Tomium Database Activity Monitor Customization Options



Note: For more information about configuring `Data Receiver Port Number` and `Plan Provider Port Number` in SecureSphere, see Adding a SecureSphere Agent for DB2 z/OS Listener on page 79.

2. Specify the values for the parameters. (You can reset all the parameters to SecureSphere Agent for z/OS defaults at any time by typing **DEFAULT** on the command line and pressing Enter.)
3. Press Enter.
4. Type **End** on the command line and press Enter or press the appropriate function key.

If you will be running multiple SecureSphere Agent for DB2 z/OSs on different LPARs, you can override the Product Load Library and the Options Module Name so that you can specify or change the customization parameters without leaving the panel.

Value You Want to Change on the Panel	Action to Take
Product Load Library	Specify the following command on the command line. NEWLIB *?neonhlq*.LOAD Press Enter Result: The Product Customization Facility displays a confirmation dialog. Press Enter again. Result: The Product Customization Facility redisplays the panel with the new library name in the Product Load Library field.
Options Module Name	Specify the following command on the command line. NEWOPT *?name* Press Enter Result: The Product Customization Facility displays a confirmation dialog. Press Enter again. Result: The Product Customization Facility redisplays the panel with the new module name in the Options Module Name field.

Detailed Information About the Customization Parameters

The table provides detailed information about the customization parameters.

Parameter	Description	Default Value
Message Data Set Name	The name of the data set that contains SecureSphere Agent for z/OS message descriptions.	*?neonhlq*.MSG
Message Language	The language for the messages ENU (U.S. English) is the only valid value for this version of SecureSphere Agent for z/OS.	ENU
Message Set	The name of the message set to be used by SecureSphere Agent for z/OS NSU01 is the only valid value for this version of SecureSphere Agent for z/OS.	NSU01
Sysout (NSUPRINT) Message Level	The detail level for messages issued by SecureSphere Agent for z/OS Specify a numeric value between 1 and 3. 1—Least verbose. Only severe messages are displayed. 2—Verbose. Severe and warning messages are displayed. 3—Most verbose. All messages are displayed.	2
Package Collection ID	The collection ID All packages required for the audit extractor should be bound using the same collection ID. Specify a collection ID for the bound that is from 1 to 8 alphanumeric characters in length. This ID must be unique to the agent instance. **Note:** Make a note of this field because you will need it again later in the configuration process.	NSUD210

Parameter	Description	Default Value
SQL Retry Delay	Indicates the number of seconds that any component of SecureSphere Agent for DB2 z/OS should wait before retrying the operation if it encounters a time out condition. Specify a numeric value between 0 and 9999.	1
Number of SQL Retries	The number of times that any component of SecureSphere Agent for DB2 z/OS will retry an SQL operation before failing. Specify a numeric value between 0 and 9999	5
-DISPLAY LOCKS for -913 Retries	Indicates the action SecureSphere Gateway takes for locks for -911 and -913 retries. If a time out condition occurs, the extractor can issue a -DISPLAY LOCKS command to DB2. The output from the command appears in NSUPRINT. Specify either: N—Never display locks. R—Display locks at each retry. F—Display locks only when the operation fails.	N
Inactivity Disconnect Timeout	Specifies a communications timeout value in seconds for the collector If this length of time is reached without any interaction with the SecureSphere Gateway, the connection will be dropped and retried. The value that you specify should be set to a multiple of the heartbeat values used by the SecureSphere Gateway. If the value is set to 0, the timeout is disabled. Specify a numeric value between 1 and 6000.	300
Data Receiver Port Number	The port number that the SecureSphere Gateway uses to receive the audit data from the collector. You must define the same port number using `impcfg`. For more information, see ***SecureSphere Administration Guide***. Specify a value from 1 to 65535. **Note:** For more information about how to configure this in SecureSphere, see Adding a SecureSphere Agent for DB2 z/OS Listener on page 79.	17671
Data Receiver Host Name	The domain name or the IP address that the SecureSphere Gateway uses to receive the audit data from the collector. You must define the same IP address using `impcfg`. For more information, see ***SecureSphere Administration Guide***.	There is no default value.
Plan Provider Port Number	The port number of the SecureSphere Gateway that provides the collection rules to SecureSphere Agent for DB2 z/OS. **Note:** SecureSphere Agent for DB2 z/OS policies are defined on the SecureSphere Management Server, but they are sent to SecureSphere Agent for DB2 z/OS from the SecureSphere Gateway (see***SecureSphere User Guide***). Specify a value from 1 to 65535. **Note:** For more information about how to configure this in SecureSphere, see Adding a SecureSphere Agent for DB2 z/OS Listener on page 79.	17670

Parameter	Description	Default Value
Plan Provider Host Name	The domain name or the IP address of the SecureSphere Gateway that provides the collection rules to SecureSphere Agent for DB2 z/OS. **Note:** SecureSphere Agent for DB2 z/OS policies are defined on the SecureSphere Management Server, but they are sent to SecureSphere Agent for DB2 z/OS from the SecureSphere Gateway (see ***SecureSphere User Guide***).	There is no default value.
Max Dataspace Size	The maximum size allocation, in megabytes, for the data collection dataspace. Specify a numeric value between 1 and 2047.	100
Local Rules Dataset Name	The fully qualified name of the data set used for the local copy of the rules (each SecureSphere Agent for z/OS started task has its own local copy of the rules data sets). Specify any valid dataset name that complies with your site naming requirements. It is recommended that the LPAR is included as a node in the dataset name.	There is no default value.
DB2 Version 8 LOAD Library	Data set name for the DB2 version 8 LOAD library. This data set name is obtained from the DB2 started task. Provide an appropriate LOAD library for each DB2 version used for audited subsystems.	There is no default value.
DB2 Version 9 LOAD Library	Data set name for the DB2 version 9 LOAD library This data set name is obtained from the DB2 started task. Provide an appropriate LOAD library for each DB2 version used for audited subsystems.	There is no default value.
DB2 Version 10 LOAD Library	Data set name for the DB2 version 10 LOAD library This data set name is obtained from the DB2 started task. Provide an appropriate LOAD library for each DB2 version used for audited subsystems.	There is no default value.
Resolve Group Attach Name	For the DB2 subsystems that you specify with the DB2 Subsystems Selected for Audit parameter, specifies whether or not group attach names should automatically resolve to all members of the data sharing group. Y - Resolve group attach names to all members. N - Use N if a data sharing member subsystem name is the same as the group attach name. The group is not audited.	Y
DB2 Subsystems Selected for Audit	One or more DB2 subsystem IDs (or data sharing group attach names) to be audited Separate multiple subsystem IDs by commas. Do not use spaces between subsystem IDs and commas. A space terminates the comma-delimited subsystem list. You can specify that SecureSphere Agent for DB2 z/OS gathers data for a maximum of 250 DB2 subsystems or members of a data sharing group. If you have more than 250, you can start another SecureSphere Agent for DB2 z/OS but you must also be sure that each DB2 subsystem is specified for only one of SecureSphere Agent for DB2 z/OSs.	There is no default value.

Completing the Configuration

This topic contains information about the tasks you must complete to finish configuring SecureSphere Agent for DB2 z/OS outside of the Product Customization Facility.

Binding Packages for the Product

The product requires that you perform a DB2 bind on those packages it uses during the audit process. You must perform a DB2 bind if you are:

- installing the product for the first time
- upgrading to a new version or release of the product
- installing maintenance and one or more of the packages have changed

Follow this process to bind the packages.

1. Locate the NSU1000 member in the ?hlq.CNTL data set.
2. Modify the sample JCL using the instructions included in the member.
3. Submit the job.
4. Verify that the job competed successfully and that all the return codes were zero.

Determining the Remaining Tasks to Complete for the Started Task

The remaining information in this topic covers the tasks that you must complete for the started task. You must complete all the remaining tasks in this topic if you are:

Installing the product for the first time

Upgrading to a new version or release of the product and you want to use a new started task (You do not have to complete these if you want to use the existing started task.)

Authorizing the Started Task for the Product

Before you can start the product, you must authorize:

- The user ID for the started task so that it can access the necessary data sets (such as the rules data set, the APF authorized LOAD library, and any of the remaining product libraries)
- The started task so that is can access the TCP/IP stack on z/OS

Using your security administration product (such as RACF), you should establish application profiles for the started task. For example, the started task uses TCP/IP to communicate with the data receiver. If you are using RACF, the started tasks must have an OMVS segment defined in RACF.

Granting DB2 Privileges

The started task must be granted EXECUTE authority on the NSU packages in the NSU collection. This must be done for each non-data sharing DB2 subsystem ID and for at least one member in any data sharing group. If a data sharing group has had privileges granted on a different LPAR setup, it does not need to be repeated at this stage.

1. Locate the NSU2000 member in the *?neonhlq*.CNTL data set.
2. Modify the sample JCL using the instructions included in the member.
3. If multiple non-data sharing subsystems will be supported on the LPAR, you must duplicate the GRANT step in the job for each subsystem. The table provides the descriptions for the variables in the jobs and indicates the action you take for the value in the duplicated GRANT step.

Variable	Value to Specify	Action to Take in the Duplicated GRANT Step
?*ssid*	ID of the DB2 subsystem or name of the data sharing group	Specify a GRANT step and ?*ssid* for each non-sharing DB2 subsystem.

Variable	Value to Specify	Action to Take in the Duplicated GRANT Step
?*db2exit*	Name of the library for the DB2 exit library	If the DB2 subsystem uses a different library, specify the name of the library in the GRANT step.
?*db2load*	Name of the DB2 LOAD library	If the DB2 subsystem uses a different LOAD library, specify the name of the library in the GRANT step.
?*dsntiad*	The name of the plan associated with the LMOD DSNTIAD For a default installation, it is DSNTIA*xx* where *xx* is the version (such as 81 or 91).	No change required.
?*dsnrunlb*	The name of the library where DSNTIAD resides The library must be APF authorized.	No changed required.
?*db2coll*	The name of the collection ID for NSU packages Specify the same value that you specified for the Package Collection ID customizable parameter.	No change required.
?*stcuser*	PUBLIC or to the name of the started task for SecureSphere Agent for z/OS	If you duplicate the GRANT step, do not change this value.

4. Submit the job.
5. Verify that the job competed successfully and that all the return codes were zero.

Initializing and Securing the Rules Data Set

The product uses a rules processing engine to isolate transactions to be reported from other, routine transactions. For each SecureSphere Agent for z/OS started task, the rules data set must be initialized before you can start SecureSphere Agent for DB2 z/OS or customize the rules data set.

You specified the rules data set using the Local Rules Dataset Name customizable parameter when you configured the product. Follow this procedure to initialize and secure the rules data set.

1. Locate the NSU3000 member in the *?neonhlq*.CNTL data set.
2. Modify the sample JCL using the instructions included in the member. The data set name for *?rulesdsn* must match the value specified for the Local Rules Dataset Name customizable parameter (see ***SecureSphere User Guide***) and should include the LPAR as a node in the name.
3. Submit the job.
4. Use your security administration product (such as RACF) to protect the rules data set so that only its owning started task can update it.
5. Verify that the job competed successfully and that all the return codes were zero.

Specifying the Priority Using WLM

To further optimize performance, set the Workload Manager (WLM) goal and importance of the started task equal to or higher than that of the DB2 subsystems being audited. With this priority, SecureSphere Agent for z/OS will run faster and more reliably.

Modifying the Started Task Procedure

Follow this procedure to modify the started task procedure and to copy the procedure to the SYSPROC library.

1. Locate the NSUPROC member in the ?hlq.CNTL library.
2. Modify the sample JCL using the instructions included in the member.
3. If you are using CA Detector for DB2 for z/OS, specify the COLL=2 parameter on the EXEC statement. (The COLL parameter is optional. The default is COLL=1.)
4. Copy the JCL to your SYSPROC library.

Starting, Managing, and Stopping SecureSphere Agent for DB2 z/OS

This topic contains information about starting and managing SecureSphere Agent for z/OS and includes:

- Requirements and Restrictions for Starting SecureSphere Agent for DB2 z/OS on page 189
- Modifying the Started Task Procedure and Starting the Started Task on page 189
- Using Operator Commands to Stop and Manage the Product on page 189

Requirements and Restrictions for Starting SecureSphere Agent for DB2 z/OS

SecureSphere Agent for DB2 z/OS has these requirements and restrictions.

- If you are using other DB2 monitoring or auditing products at your site, you must start SecureSphere Agent for DB2 z/OS before you start the other monitoring or auditing products.
- Do not start more than one SecureSphere Agent for DB2 z/OS to audit the same DB2 subsystem or member of a data sharing group.

Modifying the Started Task Procedure and Starting the Started Task

Follow this procedure to start the started tasks.

1. Locate the NSUPROC member in the *?neonhlq*.CNTL library.
2. Modify the sample JCL using the instructions included in the member.
3. If you are using CA Detector for DB2 for z/OS, specify the COLLID=2 parameter on the EXEC statement. The COLLID parameter is optional. The default is COLLID=1.
4. Copy the JCL to your SYSPROC library.
5. Perform the appropriate action. If you want to use:
   - SDSF, specify **/s taskname**
   - An MVS operator command, specify **S taskname** or **START taskname**

Using Operator Commands to Stop and Manage the Product

The table below describes the MVS operator commands that you can specify from a console to manage SecureSphere Agent for z/OS. In the command example, replace *taskname* with job name assigned by MVS to the started task address space. The table shows the tasks, the commands to specify, and an example using NSUPROC as the *taskname*.

Task You Want to Perform	Command to Specify	Example
Delete the dataspace associated with the collection process for a DB2 subsystem	/F *taskname*,MAINT,DELDSP, *db2id* where *db2id* is the ID of the DB2 subsystem. **Note:** Before you can delete the dataspace, you must terminate collection of the audit data using the TERM command shown below in this table.	/F NSUPROC,MAINT, DELDSP,DB2A
Resize the dataspace associated with the collection process for a DB2 subsystem (If the change is permanent, you must update the Max Dataspace Size customization parameter using the Product Customization Facility.)	/F *taskname*,MAINT,RSZDSP, *db2id,nnnn* Where: *db2id* is the ID of the DB2 subsystem *nnnn* is a number between 1 and 2047	/F NSUPROC,MAINT, RSZDSP,DB2A,500
Resize the dataspace associated with the collection process for all DB2 subsystems (If the change is permanent, you must update the Max Dataspace Size customization parameter using the Product Customization Facility.)	/F *taskname*,MAINT,RSZDSP, ALL,*nnnn* Where *nnnn* is a number between 1 and 2047.	/F NSUPROC,MAINT, RSZDSP,ALL,500
Set the verbosity level (*n*) of the messages that appear in //NSUPRINT	/F *taskname*,MSGLVL,*n* Where n is 1, 2, or 3 with 1 providing the least and 3 providing the most information.	/F NSUPROC,MSGLVL,1
Start the address space for SecureSphere Agent for z/OS	/S *taskname*	/S NSUPROC
Terminate collection of audit data for a single DB2 subsystem	/F taskname,TERM,*db2id* Where *db2id* is the specific DB2 SSID. You cannot specify a data sharing group attach name.	/F NSUPROC,TERM,DB2A
Terminate collection of audit data in all the DB2 subsystems and stop the address space for SecureSphere Agent for z/OS	/P *taskname*	/P NSUPROC
Terminate collection of audit data in all the DB2 subsystems	/F *taskname*, TERM,ALL	/F NSUPPROC, TERM,ALL

Installing SecureSphere Agent for DB2 z/OS - Version 1.3

This section contains the following information:

Configuring SecureSphere Agent for DB2 z/OS Tasks on page 173
Before Installing and Configuring SecureSphere Agent for DB2 z/OS on page 174
Downloading and Installing SecureSphere Agent for DB2 z/OS on page 177
Configuring SecureSphere Agent for DB2 z/OS (on z/OS) on page 180
Starting, Managing, and Stopping SecureSphere Agent for DB2 z/OS on page 189

Configuring SecureSphere for z/OS Tasks

The SecureSphere administrator must perform the tasks described below.

	Task Overview	For more information, see...
	Make the necessary preparations for installing SecureSphere Agent for DB2 z/OS.	Before Installing and Configuring SecureSphere Agent for DB2 z/OS on page 174
	Download and install the SecureSphere Agent for DB2 z/OS.	Downloading and Installing SecureSphere Agent for DB2 z/OS on page 177
	Configure the SecureSphere Agent for DB2 z/OS license.	Specifying the License Key on page 181
	Using `impcfg`, configure the data and configuration channels on which SecureSphere Agent for DB2 z/OS communicate with the SecureSphere gateway.	***SecureSphere Administration Guide***.
	Configure the SecureSphere Agent for DB2 z/OS.	***SecureSphere User Guide***
	Assign a DB2 SSID to a SecureSphere DB2 service.	***SecureSphere User Guide***.
	Define the objects and the events which should be monitored.	***SecureSphere User Guide***
	Apply audit policies for the events collected by SecureSphere Agent for DB2 z/OS.	***SecureSphere User Guide***.
	Monitor audits and logs.	***SecureSphere User Guide***

Before Installing and Configuring SecureSphere Agent for DB2 z/OS

There are a number of items you should verify and understand before beginning to install and configure SecureSphere agent for z/OS. This includes:

- Information You Must Have Before You Begin on page 174
- Terminology Used In This Guide on page 174
- Roles and Assignments for the Installation and Configuration on page 175
- Mainframe Software Requirements on page 176
- Security Requirements on page 176
- TCP/IP Requirements on page 177

- Optimizing Performance on page 177
- Supported Facilities on page 177

Information You Must Have Before You Begin

Verify that you have the following items:

Item	Additional Information
Credentials to access the Imperva FTP site	You use the credentials to access the FTP site and to download and install SecureSphere Agent for DB2 z/OS files.
License key for the SecureSphere Agent for z/OS	You must specify the license key when you install the SecureSphere Agent for z/OS on the z/OS host.

Terminology Used In This Guide

The product includes the following components.

- A component referred to as SecureSphere Agent for z/OS, that runs as a started task and gathers data about the DB2 subsystems being audited.
- A component referred to as the SecureSphere Gateway, that receives all the information gathered by SecureSphere Agent for z/OS.
- A component referred to as SecureSphere Management Server, that provides the collection rules to SecureSphere Agent for z/OS.

Roles and Assignments for the Installation and Configuration

Depending on the size and complexity of your IT organization, several people might contribute to the SecureSphere Agent for DB2 z/OS installation and configuration process. In most cases, these are the roles and their specific skills or knowledge.

- DB2 DBA or System Administrator
- Network Administrator
- Security Administrator
- System Programmer

The matrix shows:

- In order, the tasks that you perform during the installation and configuration (The tasks in the table are covered in the topics that follow.)
- In most cases, who in the organization will be involved in completing those tasks

Location in the Process	Installation and Configuration Task	Role			
		DB2 DBA	Network Administrator	Security Administrator	System Programmer
Before you install SecureSphere Agent for DB2 z/OS	Authorize any required TCP/IP connections and provide information that the System Programmer uses during product customization.		X		
	Define mainframe TCP/IP authority.			X	
Downloading and installing SecureSphere Agent for DB2 z/OS	Install the product by downloading a job that allocates the data sets and then copies the product libraries to z/OS.				X
Configuring SecureSphere Agent for DB2 z/OS	Specify the license key and product libraries on z/OS.				X
	Application Program Facility (APF) authorize the LOAD library and make the authorization permanent following an IPL. (You do not have to IPL the system to install the product.)				X
	Specify the customization parameters specific to DB2 (such as the load libraries for the versions of DB2).	X			X
	Specify the customization parameters specific to TCP/IP (such as the port numbers for the data receiver and plan provider).		X		X
Completing the configuration	Authorize the started task for the product so that it can access the required resources.			X	
	Bind the DB2 packages for the product .	X			
	Grant DB2 privileges to the user ID for the started task so that it can access the DB2 Catalog for any DB2 instance being audited.	X		X	
	Initialize and secure the rules data sets for the product so that it can only be modified by the started task.			X	X
	Specify a priority for the started task in Workload Manager (WLM).				X
Starting, managing, and stopping SecureSphere Agent for DB2 z/OS	Modify the started task procedure, copy the procedure to the SYSPROC library, and start the started task.				X

Mainframe Software Requirements

Before unloading and installing SecureSphere Agent for z/OS, verify that you have the following software installed and operational on your z/OS system.

- IBM z/OS version 1.8 or later (64 bit mode required)
- DB2 for z/OS version 8 or 9
- IBM TCP/IP version 3.1 or later

Security Requirements

The table lists the security requirements for SecureSphere Agent for z/OS.

Element	Security Requirement
DB2	You must authorize the started task-user ID so that it can access the DB2 Catalog for any DB2 instance being audited.
Rules data sets	You must protect the rules data sets for SecureSphere Agent for z/OS so that it can only be modified by the started task. You will specify the rules data sets using the Local Rules Dataset Name customizable parameter when you configure SecureSphere Agent for DB2 z/OS.
Started task	For the product to run successfully, you must provide SecureSphere Agent for z/OS with adequate authority to operating system and database resources. Using your security administration product (such as RACF), you should establish application profiles for the started task. For example, the started task for the product uses TCP to communicate with the Imperva. If you are using RACF, the started tasks for the product must have an OMVS segment defined in RACF.

TCP/IP Requirements

You must have TCP/IP network connections between the LPAR where auditing is performed and the SecureSphere Gateway and SecureSphere Management Server.

Before installing the product, you will need the:

- TCPIP.DATA data set name
- TCP/IP port numbers for the data receiver and plan provider
- Host name for the data receiver and plan provider
- You will also need to define mainframe TCP/IP authority.

Optimizing Performance

The product is architects for optimal performance so that auditing activities never impact normal business transaction processing. Key performance features include:

- When available, use of zip processors
- No reliance on slow, resource-intensive database trace utilities
- Off loads audit data from mainframe so that analysis, reporting, and data storage expenses are not incurred on the mainframe

Supported Facilities

The product supports the following local attach facilities for DB2 on z/OS:

- Call Attach (CAF)
- Resource Recover Services (RRSAF)
- CICS

- TSO
- IMS

The product also supports DRDA for distributed connections.

Downloading and Installing SecureSphere Agent for DB2 z/OS

This topic contains information about how to download and install SecureSphere Agent for DB2 z/OS. It includes:

- Downloading and Installing the Product on page 178
- APF Authorizing the LOAD Library on page 179
- Creating the ADMIN Library on page 179
- Including the Product Libraries in Your Disaster Recovery Plan on page 180

Downloading and Installing the Product



Note: There are two installation procedures: one for the installation of SecureSphere Agent for DB2 z/OS and another for the accumulated maintenance. You must follow both of these procedures, one after the other, in order to install SecureSphere Agent for DB2 z/OS.

The section describes the prerequisites and procedures required for downloading and installing SecureSphere Agent for DB2 z/OS and includes:

- Prerequisite for Downloading and Installing the Product or Cumulative Maintenance on page 178
- Procedure for Downloading and Installing the Product on page 195
- Procedure for Downloading and Installing the Accumulated Maintenance on page 197

Prerequisite for Downloading and Installing the Product or Accumulated Maintenance

The product is delivered as a tersed file or files that you must upload to your mainframe and then unterse. To unterse the files, you must have installed TRSMAIN V4 or above which can be downloaded from **`http://techsupport.services.ibm.com/390/trsmain.html`**.

There are different procedures for downloading the files and installing, depending on whether the database server (the mainframe) has Internet access or not.



Note: All files, except for text files, must be downloaded in binary mode.

Procedure for Downloading and Installing the Product

If the Mainframe Has Internet Access

To download the product files for an initial installation:

1. From **`\Downloads\SecureSphere_Agents\zOS\V1.3`**, download the file **`getnsu13.txt`**, a JCL file which allocates space on the mainframe for the installation files, downloads and unterses them.
2. Change the appropriate values according to the description in the file so that the values are aligned with your mainframe environment.

   Instructions for doing this are embedded as comments in the JCL.

3. Submit the job, which performs the following:
   3.1 Connects to the Imperva FTP site.
   3.2 Allocates space on the mainframe for the files to be downloaded and untersed.
   3.3 Downloads the SecureSphere Agent for DB2 z/OS files to the mainframe.
   3.4 Unterses the files and installs them.

If the Mainframe Does Not Have Internet Access

To download the product files for an initial installation:

1. On a machine that does have Internet access, from **\Downloads\SecureSphere_Agents\zOS\V1.3**, download the following files:
   - **nsualloc.txt**, a JCL file which allocates space on the mainframe for the installation files
   - **untnsu13.txt**, a JCL file which unterses the installation files
2. Change the appropriate values according to the description in both files so that the values are aligned with your mainframe environment.

   Instructions for doing this are embedded as comments in the JCL.
3. Submit the **nsualloc.txt** job on the mainframe.

   At this point, you have allocated the space for the files, and now you have to download them and transfer them to the mainframe.
4. From **\Downloads\SecureSphere_Agents\zOS\V1.3**, download the following eight (8) files:
   - **neon.nsu.cntl**
   - **neon.nsu.dbrm**
   - **neon.nsu.exec**
   - **neon.nsu.load**
   - **neon.nsu.messages**
   - **neon.nsu.mlib**
   - **neon.nsu.msg**
   - **neon.nsu.plib**
5. Copy these files to a portable device such as a USB flash drive.
6. Copy the files from the portable device to a PC located which has access to the mainframe.
7. On that PC, open a command prompt (**Start** > **Run** and enter the **cmd** command).
8. Connect to the mainframe using FTP.
9. Enter the following command:

```
ftp> BINARY
```

10. Enter the following commands, replacing **?yourhlq** by the value appropriate to your configuration:

```
Put neon.nsu.cntl       '?yourhlq.CNTL'       REPL
Put neon.nsu.dbrm       '?yourhlq.DBRM'       REPL
Put neon.nsu.exec       'yourhlq.EXEC'        REPL
Put neon.nsu.load       '?yourhlq.LOAD'       REPL
Put neon.nsu.messages   'yourhlq.MESSAGES'    REPL
Put neon.nsu.mlib       '?yourhlq.MLIB'       REPL
Put neon.nsu.msg        'yourhlq.MSG'         REPL
Put neon.nsu.plib       '?yourhlq.PLIB'       REPL
```

11. On the mainframe, submit the **untnsu13.txt** job.

This unterses the installation files you copied to the mainframe in the previous step.

Procedure for Downloading and Installing the Accumulated Maintenance

If the Mainframe Has Internet Access

To download the maintenance files for an existing installation:

1. From **\Downloads\SecureSphere_Agents\zOS\V1.3\Accum**, download the file **getnsu1m.txt**.
2. Change the appropriate values according to the description in the file so that the values are aligned with your mainframe environment.

   Instructions for doing this are embedded as comments in the JCL.
3. Submit the job, which performs the following:
   - 3.1 Connects to the Imperva FTP site.
   - 3.2 Allocates space on the mainframe for the maintenance files to be downloaded and untersed.
   - 3.3 Downloads the maintenance files to the mainframe.
   - 3.4 Unterses the files and installs them.

If the Mainframe Does Not Have Internet Access

1. On a machine that does have Internet access, from **\Downloads\SecureSphere_Agents\zOS\V1.3**, download the following files:
   - **nsuallma.txt**, a JCL file which allocates space on the mainframe for the maintenance files
   - **untnsu1m.txt**, a JCL file which unterses the maintenance files
2. Change the appropriate values according to the description in both files so that the values are aligned with your mainframe environment.

   Instructions for doing this are embedded as comments in the JCL.
3. Transfer the **nsuallma.txt** file to the mainframe and submit the job.

   At this point, you have allocated the space for the maintenance files, and now you have to download them and transfer them to the mainframe.
4. From **\Downloads\SecureSphere_Agents\zOS\V1.3\Accum**, download the following five (5) files:
   - **neon.nsu.acumcntl**
   - **neon.nsu.acumdbrm**
   - **neon.nsu.acumexec**
   - **neon.nsu.acumload**
   - **neon.nsu.acummsg**
5. Copy these files to a portable device such as a USB flash drive.
6. Copy the files from the portable device to a PC located which has access to the mainframe.
7. On that PC, open a command prompt (**Start** > **Run** and enter the **cmd** command).
8. Connect to the mainframe using FTP.
9. Enter the following command:

```
ftp> BINARY
```

10. Transfer the maintenance files from the PC to the space you allocated for them earlier in this procedure.
11. On the mainframe, submit the **untnsu1m.txt** job.

    This unterses the maintenance files you copied to the mainframe in the previous step.

APF Authorizing the LOAD Library

The product uses dataspaces, cross memory services, and other functions that require APF authorization. These are common and necessary requirements of system level software. The library that contains SecureSphere Agent for z/OS LOAD modules (*?neonhlq*.LOAD) must be APF authorized.

You must also ensure that the authorization is permanent to prevent losing authorization at your next IPL.

To APF authorize the LOAD library, your system programmer must issue an APF command. The table shows examples of the commands.

Status of the Data Set for the LOAD Library	Example Command
Managed by the IBM System Management Service (SMS)	SETPROG APF,ADD,DSNAME=*?neonhlq*.LOAD,SMS
Not managed by SMS	SETPROG APF,ADD,DSNAME=*?neonhlq*.LOAD,VOLUME=*volume*

Once the LOAD library has been APF authorized, updates or changes made to the configuration using the Product Customization Facility must be done by someone with authority to update an APF authorized library. (This is typically not a DBA.)

Creating the ADMIN Library

The product uses an administration (ADMIN) library to manage and maintain product keys and the associated product libraries. You must allocate and catalog this ADMIN library.



Note: If you have other NEON products installed at your site, you cannot use an existing ADMIN library. You must create a new ADMIN library with a new data set name.

Follow this process.

1. Locate the ALLOCATE member in the *?neonhlq*.CNTL data set.
2. Modify the sample JCL using the instructions included in the member.
3. Submit the job to allocate the library.

   Result: The job allocates a data set with the format shown in the following table:

Item	Value
Data set format	Partitioned data set (PDS)
Record format	Fixed block (FB), 80-character logical records LRECL=80, RECFM=FB,*blksize* Where *blksize* is your site standard block size.
Allocated space	Two tracks and 10 directory blocks

Including the Product Libraries in Your Disaster Recovery Plan

The product includes the data sets listed in the table below. These resources should also be included in your backup and disaster recovery plan.

Data Set Name	Description
?neonhlq.ADMIN	This library contains product keys.

Data Set Name	Description
?neonhlq.CNTL	This library contains the control members for SecureSphere Agent for z/OS, including sample JCL.
?neonhlq.DBRMLIB	This library contains the DB2 definitions for SecureSphere Agent for z/OS.
?neonhlq.EXEC	This library contains the REXX executables needed to configure SecureSphere Agent for z/OS.
?neonhlq.LOAD	This library contains the executable LOAD modules needed to execute SecureSphere Agent for z/OS.
?neonhlq.MESSAGES	This library contains descriptions for product messages.
?neonhlq.MLIB	This library contains messages issued by the ISPF interface.
?neonhlq.MSG	This library contains the message modules used by SecureSphere Agent for z/OS.
?neonhlq.PLIB	This library contains ISPF panels used by SecureSphere Agent for z/OS.

Configuring SecureSphere Agent for DB2 z/OS (on z/OS)

This topic contains information about using the Product Customization Facility to configure SecureSphere Agent for DB2 z/OS and includes:

- Accessing the Product Customization Facility on page 180
- Specifying the License Key on page 181
- Specifying the Product Libraries on page 182
- Specifying the Customizable Parameters on page 182
- Detailed Information About the Customization Parameters on page 184
- Completing the Configuration on page 187
- Binding Packages for the Product on page 206
- Granting DB2 Privileges on page 187
- Initializing and Securing the Rules Data Set on page 188

Accessing the Product Customization Facility

Follow this process to access the Product Customization Facility.

At the TSO prompt (option 6), specify the following command.

```
EX '?neonhlq.EXEC(NEONCNTL)' '?neonhlq'
```

Where *?neonhlq* is the high-level qualifier for SecureSphere Agent for z/OS LOAD library that you specified when you installed SecureSphere Agent for z/OS.

Result: The product displays the Product Customization Facility menu.

```
                NEON Product Customization          Row n to n of n
Command ===> _____________________________________ Scroll ===> CSR

   Product load library. . . ?neonhlq.LOAD

Type S to select a product for customization, B to BROWSE the $README member

   Product Name / Description                              Version
 _ License Management                                      nn.nn.nn
```

Specifying the License Key

You received a password for SecureSphere Agent for DB2 z/OS when you purchased SecureSphere Agent for z/OS. This password is your license key and the license key is required to run SecureSphere Agent for z/OS and protects the software from unauthorized use.

Manage Product Keys must be performed when product is initially installed, and when new keys are added or old keys are removed. If the proper product keys are not present SecureSphere Agent for z/OS will fail.Follow this process to specify the license key.

1. Type **S** next to License Management.
2. Press Enter.
3. On the NEON Enteprise Software Product Key Update panel, specify:
4. **Y** in the Manage Product Keys field
5. **Y** in the Manage Product Libraries field
6. Press Enter.

   Result: The panel redisplays with these values:

Field	Description
Product Name	Name of the family of products for this key
CPU Id	Processor id for which this key is valid
Expires	Expiration date for this key
Features	All feature codes in the key

7. Type **End** on the command line and press Enter or press the appropriate function key.

   Result: The Product Customization Facility displays the next Enterprise Software Product Key Update panel in the series.

Specifying the Product Libraries

Manage Product Libraries must be performed when SecureSphere Agent for z/OS is initially installed, and when a new installation product LOAD library is added to your system. This step ensures that there is a locator module in SecureSphere Agent for z/OS LOAD library. (The locator module indicates where the license keys are stored.) Without this module SecureSphere Agent for z/OS will not be able to perform product key validation and SecureSphere Agent for z/OS will fail. Follow this procedure to specify SecureSphere Agent for z/OS libraries.

1. On the NEON Enteprise Software Product Key Update panel, specify:
   1.1 The fully qualified data set name of the ADMIN library that you allocated in the NEON Administration Library field (Do not specify quotes around the name.)
   1.2 Your license key in the Product Key field
2. Press Enter.
3. Verify that the Status column displays Locator correct.
4. Type **End** on the command line and press Enter or press the appropriate function key.

   Result: The Product Customization Facility redisplays the Product Customization Facility menu.

   The table describes the remaining fields on the panel.

Field	Description
LC	Use this field to update (U) or delete (D) libraries.
Product Library	Lists the NEON Enteprise Software product LOAD libraries contained in the ADMIN data set library. Each library contains a locator module, which identifies the location of the ADMIN library.
Status	Describes the status of the locator module

Specifying the Customizable Parameters

You must also specify the customizable parameters for SecureSphere Agent for z/OS. Follow this procedure.

1. On the Product Customization Facility menu, type **S** next to SecureSphere Agent for DB2 z/OS and press Enter.

   Result: The Product Customization Facility displays the SecureSphere Agent for DB2 z/OS **Customization Options** panel.

```
-------- NEON Database Activity Monitor Customization Options Vnn.nn.nn ------
Command ===>
                                                                More:    - +
    Product Load Library . . ?neonhlq.LOAD
    Options Module Name. . . NSUUOPT
    Note: Parameters Initialized to NEON Recommended Values

SecureSphere Agent for z/OS Database Activity Monitor Message Log Parameters:
 Message Data Set Name. . . . . --------
 Message Language . . . . . ENU                  ENU
 Message Set. . . . . NSU01                      NUS01
 Sysout (NSUPRINT) Message Level  2              1 - 3  ( 3 = Verbose )

SQL Related Parameters:
 Package Collection ID  . . . . . NSUD130        DB2 Collection Name
 SQL Retry Delay. . . . . 1                      0 - 9999 Seconds
 Number of SQL Retries. . . . . 5                0 - 9999 Attempts
 -DISPLAY LOCKS for -913 Retries. N              N - Never
                                                 R - For Every retry
                                                 F - Only for Failure

Communication Parameters:
 Inactivity Disconnect Timeout  . 300             1 to 6000 Seconds
 Data Receiver Port Number. . . .                 1 to 65535
 Data Receiver Host Name. . . . .
 Plan Provider Port Number. . . .                 1 to 65535
 Plan Provider Host Name. . . . .


General Operating Options:
 Max Dataspace Size . . . . . 100                1 to 2047 Megabytes
 Local Rules Dataset Name . . . .

DB2 Environment Information:
 DB2 Version 8 Load Library . . .
 DB2 Version 9 Load Library . . .
 Resolve Group Attach Name. . . . Y               Y-Yes  N-No
 DB2 Subsystems Selected for Audit


Press ENTER to update END to save and exit
      CANCEL to exit ignoring any changes made since the last update
```

Figure 42 Tomium Database Activity Monitor Customization Options



Note: For more information about configuring **`Data Receiver Port Number`** and **`Plan Provider Port Number`** in SecureSphere, see Adding a SecureSphere Agent for DB2 z/OS Listener on page 79.

2. Specify the values for the parameters. (You can reset all the parameters to SecureSphere Agent for z/OS defaults at any time by typing **DEFAULT** on the command line and pressing Enter.)
3. Press Enter.
4. Type **End** on the command line and press Enter or press the appropriate function key.

   If you will be running multiple SecureSphere Agent for DB2 z/OSs on different LPARs, you can override the Product Load Library and the Options Module Name so that you can specify or change the customization parameters without leaving the panel.

Value You Want to Change on the Panel	Action to Take
Product Load Library	Specify the following command on the command line. NEWLIB *?neonhlq*.LOAD Press Enter Result: The Product Customization Facility displays a confirmation dialog. Press Enter again. Result: The Product Customization Facility redisplays the panel with the new library name in the Product Load Library field.
Options Module Name	Specify the following command on the command line. NEWOPT *?name* Press Enter Result: The Product Customization Facility displays a confirmation dialog. Press Enter again. Result: The Product Customization Facility redisplays the panel with the new module name in the Options Module Name field.

Detailed Information About the Customization Parameters

The table provides detailed information about the customization parameters.

Parameter	Description	Default Value
Message Data Set Name	The name of the data set that contains SecureSphere Agent for z/OS message descriptions.	*?neonhlq*.MSG
Message Language	The language for the messages ENU (U.S. English) is the only valid value for this version of SecureSphere Agent for z/OS.	ENU
Message Set	The name of the message set to be used by SecureSphere Agent for z/OS NSU01 is the only valid value for this version of SecureSphere Agent for z/OS.	NSU01
Sysout (NSUPRINT) Message Level	The detail level for messages issued by SecureSphere Agent for z/OS Specify a numeric value between 1 and 3. 1—Least verbose. Only severe messages are displayed. 2—Verbose. Severe and warning messages are displayed. 3—Most verbose. All messages are displayed.	2
Package Collection ID	The collection ID All packages required for the audit extractor should be bound using the same collection ID. Specify a collection ID for the bound that is from 1 to 8 alphanumeric characters in length. This ID must be unique to the agent instance. **Note:** Make a note of this field because you will need it again later in the configuration process.	NSUD130

Parameter	Description	Default Value
SQL Retry Delay	Indicates the number of seconds that any component of SecureSphere Agent for DB2 z/OS should wait before retrying the operation if it encounters a time out condition. Specify a numeric value between 0 and 9999.	1
Number of SQL Retries	The number of times that any component of SecureSphere Agent for DB2 z/OS will retry an SQL operation before failing. Specify a numeric value between 0 and 9999	5
-DISPLAY LOCKS for -913 Retries	Indicates the action SecureSphere Gateway takes for locks If a time out condition occurs, the extractor can issue a -DISPLAY LOCKS command to DB2. The output from the command appears in the NSUDLOG file. Specify either: N—Never display locks. R—Display locks at each retry. F—Display locks only when the operation fails.	N
Inactivity Disconnect Timeout	Specifies a communications timeout value in seconds for the collector If this length of time is reached without any interaction with the SecureSphere Gateway, the connection will be dropped and retried. The value that you specify should be set to a multiple of the heartbeat values used by the SecureSphere Gateway. If the value is set to 0, the timeout is disabled. Specify a numeric value between 1 and 6000.	300
Data Receiver Port Number	The port number that the SecureSphere Gateway uses to receive the audit data from the collector. You must define the same port number using `impcfg`. For more information, see ***SecureSphere Administration Guide***. Specify a value from 1 to 65535. **Note:** For more information about configuring this in SecureSphere, see Adding a SecureSphere Agent for DB2 z/OS Listener on page 79.	17671
Data Receiver Host Name	The domain name or the IP address that the SecureSphere Gateway uses to receive the audit data from the collector. You must define the same IP address using `impcfg`. For more information, see ***SecureSphere Administration Guide***.	There is no default value.
Plan Provider Port Number	The port number of the SecureSphere Gateway that provides the collection rules to SecureSphere Agent for DB2 z/OS. **Note:** SecureSphere Agent for DB2 z/OS policies are defined on the SecureSphere Management Server, but they are sent to SecureSphere Agent for DB2 z/OS from the SecureSphere Gateway (see ***SecureSphere User Guide***). Specify a value from 1 to 65535. **Note:** For more information about configuring this in SecureSphere, see Adding a SecureSphere Agent for DB2 z/OS Listener on page 79.	17670

Parameter	Description	Default Value
Plan Provider Host Name	The domain name or the IP address of the SecureSphere Gateway that provides the collection rules to SecureSphere Agent for DB2 z/OS. **Note:** SecureSphere Agent for DB2 z/OS policies are defined on the SecureSphere Management Server, but they are sent to SecureSphere Agent for DB2 z/OS from the SecureSphere Gateway (see ***SecureSphere User Guide***).	There is no default value.
Max Dataspace Size	The maximum size allocation, in megabytes, for the data collection dataspace. Specify a numeric value between 1 and 2047.	100
Local Rules Dataset Name	The fully qualified name of the data set used for the local copy of the rules (each SecureSphere Agent for z/OS started task has its own local copy of the rules data sets). Specify any valid dataset name that complies with your site naming requirements. It is recommended that the LPAR is included as a node in the dataset name. Enclose the name in quotes.	There is no default value.
DB2 Version 8 LOAD Library	Data set name for the DB2 version 8 LOAD library. This data set name is obtained from the DB2 started task. Provide an appropriate LOAD library for each DB2 version used for audited subsystems.	There is no default value.
DB2 Version 9 LOAD Library	Data set name for the DB2 version 9 LOAD library This data set name is obtained from the DB2 started task. Provide an appropriate LOAD library for each DB2 version used for audited subsystems.	There is no default value.
Resolve Group Attach Name	For the DB2 subsystems that you specify with the DB2 Subsystems Selected for Audit parameter, specifies whether or not group attach names should automatically resolve to all members of the data sharing group. Y - Resolve group attach names to all members. N - If the name is a group attach name instead of subsystem ID, do not resolve group attach names (the group is not audited).	Y
DB2 Subsystems Selected for Audit	One or more DB2 subsystem IDs (or data sharing group attach names) to be audited separated by commas and no spaces Use ALL to audit every discovered DB2 subsystem. Multiple subsystem IDs are separated by a comma. A space terminates the comma-delimited subsystem list. Separate multiple subsystem IDs by commas. A space terminates the comma-delimited subsystem list. You can specify that SecureSphere Agent for DB2 z/OS gathers data for a maximum of 250 DB2 subsystems or members of a data sharing group. If you have more than 250, you can start another SecureSphere Agent for DB2 z/OS but you must also be sure that each DB2 subsystem is specified for only one of SecureSphere Agent for DB2 z/OSs.	There is no default value.

Completing the Configuration

This topic contains information about the tasks you must complete to finish configuring SecureSphere Agent for DB2 z/OS outside of the Product Customization Facility.

Authorizing the Started Task for the Product

Before you can start the product, you must authorize:

- The user ID for the started task so that it can access the necessary data sets (such as the rules data set, the APF authorized LOAD library, and any of the remaining product libraries)
- The started task so that is can access the TCP/IP stack on z/OS

Using your security administration product (such as RACF), you should establish application profiles for the started task. For example, the started task uses TCP/IP to communicate with the data receiver. If you are using RACF, the started tasks must have an OMVS segment defined in RACF.

Binding Packages for the Product

The product requires that you perform a DB2 bind on those packages it uses during the audit process. Follow this process to bind the packages.

1. Locate the NSU1000 member in the *?neonhlq*.CNTL data set.
2. Modify the sample JCL using the instructions included in the member.
3. Submit the job.
4. Verify that the job competed successfully and that all the return codes were zero.

The started task must be granted EXECUTE authority on the NSU packages in the NSU collection. This must be done for each non-data sharing DB2 subsystem ID and for at least one member in any data sharing group. If a data sharing group has had privileges granted on a different LPAR setup, it does not need to be repeated at this stage.

1. Locate the NSU2000 member in the *?neonhlq*.CNTL data set.
2. Modify the sample JCL using the instructions included in the member.
3. If multiple non-data sharing subsystems will be supported on the LPAR, you must duplicate the GRANT step in the job for each subsystem. The table provides the descriptions for the variables in the jobs and indicates the action you take for the value in the duplicated GRANT step.

Variable	Value to Specify	Action to Take in the Duplicated GRANT Step
?*ssid*	ID of the DB2 subsystem or name of the data sharing group	Specify a GRANT step and ?*ssid* for each non-sharing DB2 subsystem.
?*db2exit*	Name of the library for the DB2 exit library	If the DB2 subsystem uses a different library, specify the name of the library in the GRANT step.
?*db2load*	Name of the DB2 LOAD library	If the DB2 subsystem uses a different LOAD library, specify the name of the library in the GRANT step.
?*dsntiad*	The name of the plan associated with the LMOD DSNTIAD For a default installation, it is DSNTIA*xx* where *xx* is the version (such as 81 or 91).	No change required.
?*dsnrunlb*	The name of the library where DSNTIAD resides The library must be APF authorized.	No changed required.

Variable	Value to Specify	Action to Take in the Duplicated GRANT Step
?*db2coll*	The name of the collection ID for NSU packages Specify the same value that you specified for the Package Collection ID customizable parameter.	No change required.
?*stcuser*	PUBLIC or to the name of the started task for SecureSphere Agent for z/OS	If you duplicate the GRANT step, do not change this value.

4. Submit the job.
5. Verify that the job competed successfully and that all the return codes were zero.

Initializing and Securing the Rules Data Set

The product uses a rules processing engine to isolate transactions to be reported from other, routine transactions. For each SecureSphere Agent for z/OS started task, the rules data set must be initialized before you can start SecureSphere Agent for DB2 z/OS or customize the rules data set.

You specified the rules data set using the Local Rules Dataset Name customizable parameter when you configured the product. Follow this procedure to initialize and secure the rules data set.

1. Locate the NSU3000 member in the *?neonhlq*.CNTL data set.
2. Modify the sample JCL using the instructions included in the member. The data set name for *?rulesdsn* must match the value specified for the Local Rules Dataset Name customizable parameter (see see***SecureSphere User Guide***) and should include the LPAR as a node in the name.
3. Submit the job.
4. Use your security administration product (such as RACF) to protect the rules data set so that only its owning started task can update it.
5. Verify that the job competed successfully and that all the return codes were zero.

Specifying the Priority Using WLM

To further optimize performance, set the Workload Manager (WLM) goal and importance of the started task equal to or higher than that of the DB2 subsystems being audited. With this priority, SecureSphere Agent for z/OS will run faster and more reliably.

Starting, Managing, and Stopping SecureSphere Agent for DB2 z/OS

This topic contains information about starting and managing SecureSphere Agent for z/OS and includes:

- Requirements and Restrictions for Starting SecureSphere Agent for DB2 z/OS on page 189
- Modifying the Started Task Procedure and Starting the Started Task on page 189
- Using Operator Commands to Stop and Manage the Product on page 189

Requirements and Restrictions for Starting SecureSphere Agent for DB2 z/OS

SecureSphere Agent for DB2 z/OS has these requirements and restrictions.

- If you are using other DB2 monitoring or auditing products at your site, you must start SecureSphere Agent for DB2 z/OS before you start the other monitoring or auditing products.
- Do not start more than one SecureSphere Agent for DB2 z/OS to audit the same DB2 subsystem or member of a data sharing group.

Modifying the Started Task Procedure and Starting the Started Task

Follow this procedure to start the started tasks.

1. Locate the NSUPROC member in the *?neonhlq*.CNTL library.
2. Modify the sample JCL using the instructions included in the member.
3. If you are using CA Detector for DB2 for z/OS, specify the COLLID=2 parameter on the EXEC statement. The COLLID parameter is optional. The default is COLLID=1.
4. Copy the JCL to your SYSPROC library.
5. Perform the appropriate action. If you want to use:
   - SDSF, specify **`/s taskname`**
   - An MVS operator command, specify **`S taskname`** or **`START taskname`**

Using Operator Commands to Stop and Manage the Product

The table below describes the MVS operator commands that you can specify from a console to manage SecureSphere Agent for z/OS. In the command example, replace *taskname* with job name assigned by MVS to the started task address space. The table shows the tasks, the commands to specify, and an example using NSUPROC as the *taskname*.

Task You Want to Perform	Command to Specify	Example
Delete the dataspace associated with the collection process for a DB2 subsystem	/F *taskname*,MAINT,DELDSP, *db2id* where *db2id* is the ID of the DB2 subsystem. **Note:** Before you can delete the dataspace, you must terminate collection of the audit data using the TERM command shown below in this table.	/F NSUPROC,MAINT, DELDSP,DB2A
Resize the dataspace associated with the collection process for a DB2 subsystem (If the change is permanent, you must update the Max Dataspace Size customization parameter using the Product Customization Facility.)	/F *taskname*,MAINT,RSZDSP, *db2id,nnnn* Where: *db2id* is the ID of the DB2 subsystem *nnnn* is a number between 1 and 2047	/F NSUPROC,MAINT, RSZDSP,DB2A,500

Task You Want to Perform	Command to Specify	Example
Resize the dataspace associated with the collection process for all DB2 subsystems (If the change is permanent, you must update the Max Dataspace Size customization parameter using the Product Customization Facility.)	/F *taskname*,MAINT,RSZDSP, ALL,*nnnn* Where *nnnn* is a number between 1 and 2047.	/F NSUPROC,MAINT, RSZDSP,ALL,500
Set the verbosity level (*n*) of the messages that appear in //NSUPRINT	/F *taskname*,MSGLVL,*n* Where n is 1, 2, or 3 with 1 providing the least and 3 providing the most information.	/F NSUPROC,MSGLVL,1
Start the address space for SecureSphere Agent for z/OS	/S *taskname*	/S NSUPROC
Terminate collection of audit data for a single DB2 subsystem	/F taskname,TERM,*db2id* Where *db2id* is the specific DB2 SSID. You cannot specify a data sharing group attach name.	/F NSUPROC,TERM,DB2A
Terminate collection of audit data in all the DB2 subsystems and stop the address space for SecureSphere Agent for z/OS	/P *taskname*	/P NSUPROC
Terminate collection of audit data in all the DB2 subsystems	/F *taskname*, TERM,ALL	/F NSUPPROC, TERM,ALL

CHAPTER 7

Gateways

This chapter describes configuration of SecureSphere gateways, and includes the following:

Configuring Gateways and Gateway Groups on page 211

Configuring Gateways and Gateway Groups

SecureSphere gateways monitor traffic, enforce policies and send events to the SecureSphere management server.

A gateway's management server is defined during the gateway's initial configuration, using **`impcfg`**.

For more information, see Configuring a Gateway on page 71.

You can configure gateways and gateway groups, as follows:

- Gateways on page 211
- Gateway Groups on page 215
- Exporting Technical Information from Gateway and Onebox on page 219

Gateways

Creating a gateway means creating a management server-gateway relationship, that is, specifying that a gateway is managed by this management server (the management server that the SecureSphere GUI is running on). This is done using **`impcfg`**.

For more information, see Configuring a Gateway on page 71.

To view a gateway:

1. In the **Main** workspace, select **Setup** > **Gateways.**
2. In the **Filter** pane, select **By Mode**, **By Platform** or **By Server Group**.
3. Select a gateway.

   The gateway's details are displayed in the **Gateway Details** pane.

To view a gateway:

1. In the **Main** workspace, select **Setup** > **Gateways.**
2. In the **Filter** pane, select **By Mode**, **By Platform** or **By Server Group**.
3. Select a gateway.

Gateway Details

Details Tab - General Info

Field	Description
Management Interface IP	The IP address of the gateway's management interface.
Installed Version	The version of SecureSPhere currently installed on this gateway.
Up Since	The date and time since which the gateway has been continuously running.
License Level	The Imperva license level (Enterprise or Standard).
Performance Report CSV	Click **Download** to export the gateway's statistics to a CSV file.

Details Tab - Group

Field	Description
Tech Info (ZIP)	Click **Download** to export gateway or one-box get tech info to a zip file. For more information see Exporting Technical Information from Gateway and Onebox on page 219.
Gateway Group	The name of the gateway group to which this gateway belongs. To move the gateway to another group, select the group from the dropdown list. **Note:** When you move a gateway from one gateway group to another, the configurations of any DB Agents running on that gateway will be lost and you will have to re-enter the configuration data (in **Main** > **Setup** > **Agents**).

The following section displays a read-only list of the errors reported for this gateway.

Detail Tab - Errors

Field	Description
Errors	A description of the error, for example, “Minimum disk space reached, data is lost.”

The following section displays options related to audit archive data generated on the gateway.

Detail Tab -Audit Archive Settings

Option	Description
Archive audit data directly from Gateway	If this option is enabled, audit data is sent from the gateway directly to the audit archive. For more information, see Configuring Archiving per Gateway on page 214. If this option is not enabled, audit data is sent from the gateway to the management server, and from there to the audit archive.

The following table displays a read-only list of the server groups which this gateway protects.

Detail Tab - Server Groups

Field	Description
Name	The name of the server group.
Status	The status of the server group (for example, “Running”).
Errors	The number of errors for the server group. Expand the server group to display a list of the errors.

The following table the CPU load on the server.

Details Tab - CPU Load

Field	Description
kernel	The CPU load of the kernel mode module.

Details Tab - CPU Load

Field	Description
user	The CPU load of the user mode module.

Remote Agent Details in the Gateways Window



Note: When you move a Gateway from one Gateway group to another (**Main** > **Setup** > **Gateways**), the configurations of any DB Agents running on that Gateway will be lost and you will have to re-enter the configuration data.

For each pre- version 7.0 Remote Agent which sends events to the Gateway, the following data is displayed.

Agents Tab in the Gateways Window

Field	Description
Name	The name of the Remote Agent.
Status	The status of the Remote Agent (for example, “Running”).
IP	The IP address of the database server on which the Remote Agent is running.
Last Seen	The date and time of the last event received from the Remote Agent.
Throughput	The Remote Agent’s throughput.
Conn / Sec	The number of connections per second handled by the Remote Agent.

For information about Remote Agent, see the Remote Agents chapter in the ***SecureSphere User Guide***.

Log Collectors Details in the Gateways Window

For each Log Collector that sends events to the gateway, the following data is displayed.

Field	Description
Log Collector	The name of the Log Collector.
Status	The status of the Log Collector (for example, “Running”).
Last Seen	The date and time of the last event received from the Log Collector.
Server Group	The name of the database server group.
Service	The name of the database service.
Events Since Up Time	The number of events since the connection to the Log Collector started.
Connections Since Up Time	The number of connections between the gateway and the Log Collector.
Too Many Logs Count	The number of times the gateway encountered too many logs (and was unable to handle all of them).
Invalid Events Count	The number of invalid events encountered in logs and discarded.

Field	Description
Invalid Logs Count	The number of logs which were completely invalid.
Failed Connection Count	The number of times the gateway failed to connect to the Log Collector.
Errors Since Up Time	The number of errors since the connection to the Log Collector started.
Unexpected Collector Terminations	The number of times the connection to the Log Collector was unexpectedly terminated.
Up Since	The date and time of the connection to the Log Collector started.
Last Event Time	The date and time of the last event received by the gateway.
Last Connection Time	The date and time of the last time the gateway retrieved a log.

For information about Log Collectors, see Log Collector chapter in the ***SecureSphere User Guide***.

Configuring Archiving per Gateway

For performance reasons, you may wish to send audit records directly from the gateway to the archive location, rather than from the gateway to the management server and from there to the archive.

To configuring archiving per gateway:

1. If you will be using NFS for the archive directory, then in **Admin** > **System Definitions** > **Action Interfaces**, create an **NFS Archive** action interface and specify a **Destination Directory**.

   Alternatively, you can use SCP for the archive directory. In this cases, the appropriate action interface are already defined.

   For information on how to create an **NFS Archive** action interface, see “Creating and Configuring Action Interfaces” in the ***SecureSphere User Guide***.
2. In **Main** > **Policies** > **Action Sets**, create an action set to be used by the archive action interface you will be using (whether NFS or SCP).

   Depending on how the action interface is configured, you may need to specify the **Destination Directory**.

   For information on how to do this, see “Creating Custom Action Sets” in the ***SecureSphere User Guide***.
3. In **Main** > **Policies** > **Audit**, under **Archiving Action** (in the **Archiving** tab), select the action set.
4. In **Main** > **Setup** > **Gateways**, select **Archive audit data directly from Gateway**.

For SCP archives, no further configuration is necessary.

For NFS archives, you must mount the archive directory to the gateway, as described below.

Mounting the Audit Archive Directory (NFS)



Note: The mounted directory must be shared.

To mount a Windows directory:

1. SSH to the gateway.
2. Execute the following command:

```
mount -t smbfs -o username=<win-user>,workgroup=IL //<win-user>/<win-dir> /
<unix-dir>
```

To mount a Linux directory:

1. Confirm that the NFS server is running on the remote machine.
2. Confirm that the directory is shared.
3. SSH to the gateway.
4. Execute the following command:

```
mount host:/dir_to_mount //local_dir
```

To mount a CentOS5 directory:

1. SSH to the gateway.
2. Execute the following command:

```
mount -t cifs -o username=<win-user>,workgroup=IL //<win-user>/<win-dir> /
<unix-dir>
```

Gateway Groups

You can view, create and edit gateway groups.

To view a gateway group:

1. In the **Main** workspace, select **Setup** > **Gateways.**
2. In the **Gateways** pane, click .
3. In the **Create New Gateway Group** window, enter the following data:

Name	The name of the gateway group.
Platform	Select a platform from the menu: • **Imperva** • **Imperva G2** • **Crossbeam** • **Other**
Gateway Mode	Select a mode from the menu: • **STP Bridge** • **IMPVHA Bridge** • **Sniffing** • **Reverse Proxy Apache** • **Reverse Proxy Kernel** For information abut these modes, see Configuring a Gateway on page 71.

Fail Mode	Select a **Fail Mode**: • **Fail Open**: In the event the gateway fails, it will continue to pass traffic without monitoring it. • **Fail Close**: In the event the gateway fails, it will block all traffic. • **High Availability**: This gateway group is a high availablility cluster. This option is available only if **Gateway Mode** is **STP Bridge**. You must also toggle high availability for each of the gateways in the group using `impcfg` (**Top** > **Gateway**> **Interfaces** > **Toggle HA on a bridge**).
Overload Policy	Select **Block on Overload** to specify that if the gateway's throughput capacity is exceeded, all connections will be blocked until the throughput falls. A gateway is considered overloaded when any of the following occurs: • CPU or memory utilization reach 100%. • Throughput exceeds the defined limit. • Resources are exhausted.

4. Click **Create**.
5. Click **Save**.

To view a gateway group:

1. In the **Main** workspace, select **Setup** > **Gateways.**
2. In the **Filter** pane, select **By Mode**, **By Platform** or **By Server Group**.
3. Select a gateway group.
   The gateway group's details are displayed in the **Gateway Group Details** pane.

To edit a gateway group:

1. In the **Main** workspace, select **Setup** > **Gateways.**
2. In the **Filter** pane, select **By Mode**, **By Platform** or **By Server Group**.
3. Select a gateway group.
4. In the **Gateway Group Details** pane, enter the following data:

General Info	
Name	The gateway group's **Name** is displayed. You can change **Name** here.
Platform	The gateway group's **Platform** is displayed.
Topology Configuration	
Mode	The gateway group's **Mode** is displayed.
Fail Mode	Select a **Fail Mode**: • **Fail Open**: In the event the gateway fails, it will continue to pass traffic without monitoring it. • **Fail Close**: In the event the gateway fails, it will block all traffic. **Note: Fail Open** is not supported for 10G appliances.
Overload Policy	Select **Block on Overload** to specify that if the gateway's throughput capacity is exceeded, all connections will be blocked until the throughput falls.
Reset untraceable user connections	FAM only - Select **Reset untraceable user connections** to specify that the SecureSphere Gateway should reset connections that were opened before the Gateway was started, so that the actual user will be identified in the audit file.
Allow Ambiguous Packets	
Allow IP bad checksum	Allow a packet through the gateway even if it has a bad IP checksum.
Allow TCP bad checksum	Allow a packet through the gateway even if it has a bad TCP checksum.
Allow TCP reset out-of-window	
Allow TCP sequence before ISN	Allow a packet through the gateway even if its sequence number is less than the TCP session's ISN (Initial Sequence Number).
Allow TCP ack beyond sequence	
Allow TCP sequence out-of-window	
Allow UDP bad checksum	Allow a packet through the gateway even if it has a bad UDP checksum.
External Logger	
Syslog transport	Select a transport protocol for issuing logs to syslog: • **UDP**: The connectionless UDP protocol is used. UDP carries less overhead but has the disadvantage that delivery is not guaranteed. • **TCP**: The TCP protocol is used. TCP carries a higher overhead than UDP but delivery is guaranteed. Some additional configuration may be necessary.

Primary Host	The IP address of the primary host to which syslogs will be sent.
Port	The port on the primary host to which syslogs will be sent.
Secondary Host	The IP address of the secondary host to which syslogs will be sent.
Port	The port on the secondary host to which syslogs will be sent.
Performance Profiling	
Enable	Check **Enable** to monitor the performance of this gateway in the **System Performance** window (see Chapter 15, System Performance).
Gateways	
Gateways	In the **Gateways** section, a read-only list of the gateways which are members of this group is displayed. If you have made any changes in the **Gateway Group Details** pane, click **Save**.

Exporting Technical Information from Gateway and Onebox

On occasion, when encountering trouble with SecureSphere operation, Imperva support may request that you provide them with technical information that is automatically generated by SecureSphere, so they can analyze logs and other information. You can export this information from the SecureSphere gateway using the GUI. This procedure describes how to export tech info for a SecureSphere Gateway from the GUI. For information on exporting tech info for SecureSphere Management Servers, see Exporting Technical Information from Management Servers on page 332

To export technical information for a Gateway:

1. In the **Main** workspace, select **Setup** > **Gateways.**
2. In the **Gateways** pane, select the **Gateway** whose get tech info you want to export.



Note: The Gateway must be in the status Running.

3. In the **Details** pane, next to **Tech Info (zip)**, click **Download**.

   SecureSphere prepares the information for download. Once complete a dialog box appears with a link. Click the link and download the zip file to the desired location. You can then mail it to Imperva support for analysis.



Note: When exporting technical information from a Onebox architecture, both Gateway and Management Server technical information is exported.

CHAPTER 8

Licenses

Imperva SecureSphere requires a license. This chapter describes the SecureSphere licensing process and reviews the following subjects:

License Overview on page 221
Uploading Licenses on page 222
Viewing Licenses on page 223
Managing Database Scanning and Assessment Licenses on page 225

License Overview

A license contains the following information:

- product information - a list of the products enbaled by the license, for example, Web, DB, File, etc.
- gateway modules - the types of gateway (for example, WAF, DMA/DBF, etc.) enabled by the license and counters for each module (specifying the number of modules enabled)
- assessment counter - the number of scanned servers enabled
- File / URM - the number of users enabled
- Expiration date - for evaluation licenses only; non-evaluation licenses are not time-limited
- Maintenance period - specifying the period during which ADC content can be downloaded

When a license is renewed, it is replaced by a new license.

Licenses for a SecureSphere management server and all the gateway it manages are installed on the management server.

Uploading Licenses

To upload a license:

1. In the **Admin** workspace, click **Licensing**.
2. Click **Actions**.
3. From the menu, select **Upload License File**.
4. In the Upload License File window, click **Browse** and navigate to the license file.

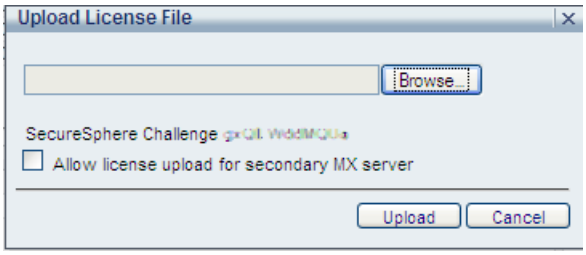


Figure 43 Upload License File Window

5. If this is an MX-HA depoyment, enable **Allow license upload for secondary MX server**.
6. Click **Upload**.

Viewing Licenses

To view all the installed licenses:

1. In the **Admin** workspace, click **Licensing**.

   A summary of the installed licenses is displayed in the **License** pane.

   Under **License Summary**, the following information is displayed:

   - **Level**: **Standard Edition** or **Enterprise Edition**.
   - **Products**: A list of licensed products, for example, **WAF** (Web Access Firewall), **DAS** (Discovery and Assessment Server), Database Scanning and File Server Scanning and ThreatRadar.

   Under **License Summary (GW modules)**, the following information is displayed for each gateway license:

   - **Module**: The Imperva product, for example DAS, DAM, *etc*.
   - **Quantity**: The number of modules included in the license.
   - **HW**: The gateway hardware model, for example, **G4** or **G10**.
   - **File**: The name of the license file which contains this gateway license.
   - **Expiration Date**: The date this gateway license expires.

   Under **License Summary (Cross System modules)**, information is displayed about the Imperva Customer Service support license, including ADC content:

   - **Module**: For example, ADC Content, Maintenance, *etc*.
   - **Start Date**: The date from which the license is valid.
   - **Expiration Date**: The date the license expires.

   Under **License files**, the following information is displayed for each license file:

   - **File Name**: The name of the license file.
   - **License Type**: The type of license, for example, evaluation.
   - **Issuing Date**: The date the license was issued.
   - **Comments**: Other information.

2. Select a license file from among those displayed under **License files**.

   The details of the licenses contained in the selected file are displayed in the right pane, under **Details**.

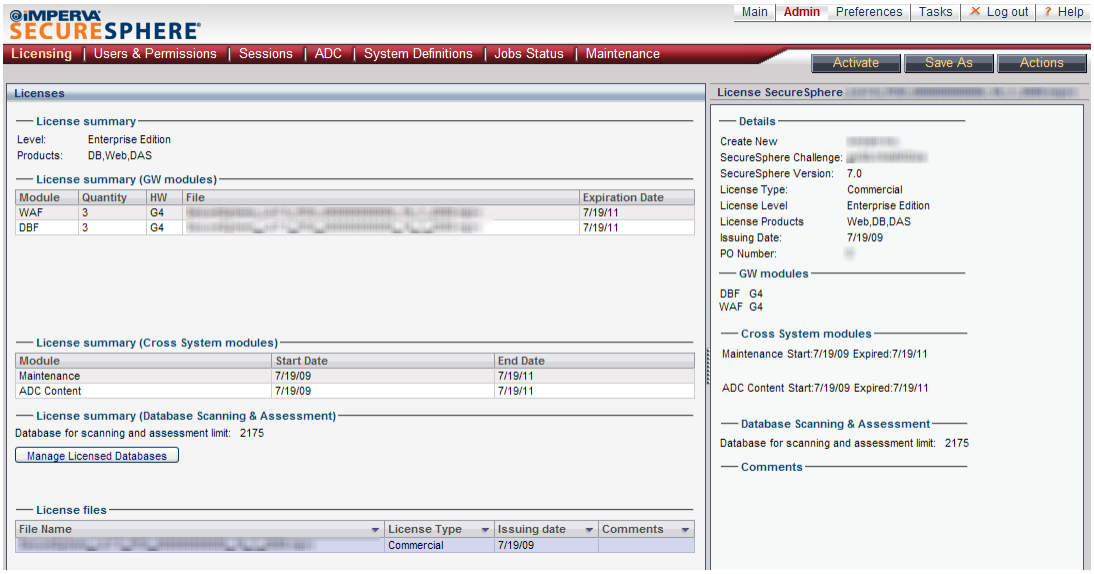


Figure 44 Licenses Window



Note: Some information about the license is displayed in the SecureSphere login screen.

Managing Database Scanning and Assessment Licenses

SecureSphere is licensed with a pre-defined number of assets that can be scanned and assessed based on gateway modules. Once you start running assessments on assets, available licenses are automatically assigned. For every new asset, a new entry is added to the table in the Manage Licensed Databases window described below. This procedure describes how to manage these licenses after they have already been assigned.

To manage licenses for database scanning and assessment:

1. In the **Admin** workspace, click **Licensing**. Currently installed licenses are displayed.
2. In the **License Summary (Database Scanning & Assessment)** pane, click **Manage Licensed Databases**. The **Managed Licensed Database** window appears.
3. From the **Status** dropdown menu in the **Managed Licensed Databases** window, select the desired option:
   - **Licensed**: Assigns a license to the selected item.
   - **Unlicensed**: Removes a license from the selected item. The next time an assessment is run on this item, the SecureSphere management server will check if there is available license. If there is, it changes its status to “Licensed” and assesses the database. If there is no license available, it will remain unlicensed and any attempt of assessment results in an error.
   - **Ignore**: Ignores the selected item (doesn’t attempt to assess it).
4. At the bottom of the **Managed Licensed Databases** window, click **Save**. Your changes have been saved.



Note: To remove an entry from the table and free up a license, select the item in the table and then click the **Delete** icon.

CHAPTER 9

Users and Permissions

SecureSphere provides a robust permissions model that enables you to create new users, assign them one or more roles that grant permissions to objects based on those roles, then grant users additional permissions to specific objects in SecureSphere.

This chapter describes how to manage SecureSphere users and contains the following sections:

Understanding Permissions on page 228
Permissions Workflow on page 233
Working with Roles on page 234
Working with Users on page 237

Understanding Permissions

This section provides information about the mechanism for managing users and permissions and the impact of granting or removing permissions. It reviews the following subjects:

- Permission Models in SecureSphere on page 228
- Roles and Users on page 228
- Permission Types on page 229
- Understanding the Permissions Window on page 231
- Adding and Removing Permissions on page 232
- Notes on Permission Behavior on page 232

Permission Models in SecureSphere

It is recommended that before you get started in creating roles and users you first determine how to best match your user model with your workflow. There are three primary models that are recommended to understand how to match SecureSphere users with your organization.

Table 2

Based on:	
Role Based	In this model, users are assigned a specific role and receive permissions for fulfilling this role. For example, perhaps a user is designated specifically to monitor a certain type of traffic. You would assign them the role of Web or DB Administrator based on what kind of traffic they are responsible for.
Product Line Based	In this model, a user may be responsible for all aspects of a specific product line, either Web based or database based products. For example, they may be responsible for the configuration of security policies for that product, the monitoring of traffic, and the creation of reports. You would then create a user and assign them the various role for that product, or create a new role for this purpose and configure it as required.
Specific Access Based	In some cases you may want to give targeted permissions to an outside user. For example, if you are an ISP and want to give your customers the ability to only view the specific web service and monitor that service, you would create a user for this purpose, and only grant him permissions to view the specific objects related to the service. In some cases you may want to give targeted permissions to a user. In that case, you need to create a user for this purpose, and grant him only specific permissions.

Roles and Users

The permissions model in SecureSphere is based on the following primary types of permissions:

- **Roles**: Represents a role in an organization, such as a Web Security Administrator and includes a set of permissions specified for that role. SecureSphere comes with a set of pre-defined roles.
  For information on roles see Working with Roles on page 234

  For a list of predefined roles and their descriptions see PreDefined Roles on page 234

- **External Roles**: Represents a group of users defined in an external authorization system (currently Active Directory only). In SecureSphere these roles are mapped to the roles in external systems and can receive SecureSphere roles and permissions, similarly to SecureSphere users. For more information on external roles see the User Guide.
- **Users**: Represents an actual user in SecureSphere to whom permissions are granted. When users are created, they are assigned one or more roles, granting them the permissions associated with those roles, and can additionally be assigned permissions to specific users. For more information on users see Working with Users on page 237
- **External Users**: A user that is defined in the external authorization system (currently Active Directory only) and in SecureSphere this user is created automatically during user's first login. Such user cannot be deleted or assigned roles in SecureSphere, only in the external system. External users can receive SecureSphere permissions, granted explicitly by Administrator, or automatically when it creates objects. For more information on external users see the User Guide.

Permission Types

There are three primary types of permissions that users can be granted to various SecureSphere components. These include the following:

Table 3

Based on:	Description
View	Enables users to only view the specific object. Though users cannot edit their parameters nor create new objects. If a user doesn't have "view" permission to an object, they can still see the object's name.
Edit	Enables users to view a specific object, edit the details of an object (asset configuration, policy rules etc.), but not create new objects.
Create	Enables users to create objects (per category). These users then automatically receive edit and view permissions for this object. A category Subsystem on SOM controls all the permissions that SOM users are granted to work with MXs on that SOM.

Working with the Subsystem category objects on SOM:

- When you have **View** permissions, you can perform the following with MXs registered to that SOM:
  - Viewing MXs in the **Registered MXs** window.
  - Viewing MXs in the **Apply to MXs** pane that presents the items that can be downloaded to MXs.
  - Viewing the statistical data from that MX in the **Dashboard**.
- When you have **Create** permission for MXs, you can create MXs.
- When you have **Edit** permissions, you can perform the following with MXs registered to that SOM:
  - Editing MX properties.
  - Registering an MX, deleting an MX and test connection to that MX.
  - Drilldown to that MX.
  - Downloading items to that MX.

In addition to the permissions mentioned above, all users can use all objects available in SecureSphere such as policies, global objects, action sets, etc., on assets they have permissions to. For example, if a user has edit permissions to a specific web service, they can apply any existing policy to that web server, even if they don't have view permissions on the policy.

Understanding the Permissions Window

To access permissions:

1. From the **Admin** workspace, click **Users & Permissions**.
2. Select a user or group.

   For information on how to create users, see Creating a SecureSphere User on page 237.

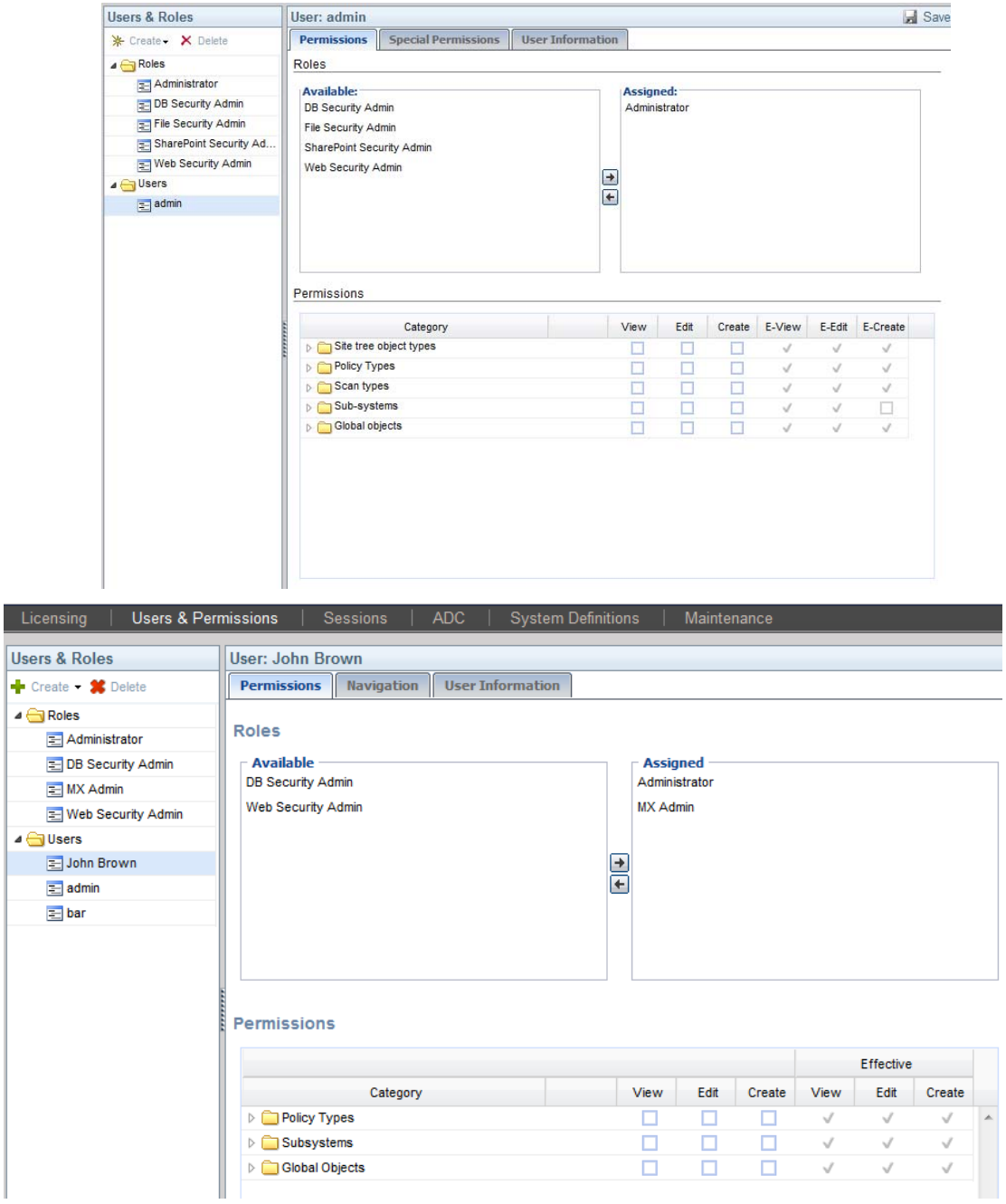


Figure 45 Permissions Window Displaying User Permissions

Adding and Removing Permissions

Adding and removing permissions to objects in the permissions window is accomplished by selecting or deselecting the relevant checkbox then clicking Save. Permissions are granted to the specific object or category selected.



Note: When permissions are granted to categories, they automatically cascade to all objects in that category. The category object is selected, though the its objects appear disabled.

Notes on Permission Behavior

Granting or revoking permissions in SecureSphere affects various permission objects in different ways. The below provides some important information regarding permission behavior to assist in better understanding and managing permissions.

- The default user is “administrator”. The Administrator user has create, view and edit permissions to the entire SecureSphere system.
- Only Administrators or users assigned the **Administrator** role, have access to the **Admin** workspace.
- A regular user has edit permission for any objects they create, except if an Administrator later revokes those permissions.
- When enabling Edit permissions, uses are automatically granted view permissions.

Permissions Workflow

The basic process of creating users and assigning permissions includes the following primary steps:

Table 4

#	Action	Description	For more information, see...
1	Create or customize roles as desired	Customize existing roles or create new roles to match your organization's needs.	Working with Roles on page 234
2	Create a new user	Create a new user to represent a SecureSphere user that needs access.	to create a separate ex role, which is like user
3	Assign roles to the user	Assign the desired roles to the user that match that user's responsibilities.	Assigning Roles to Users on page 238
4	Configure object specific permissions	Configure any additional permissions for specific objects the user or role might require, if applicable.	Configuring Object or Category Level Permissions on page 238
5	Configure navigation and activate settings permissions	Configure permissions for access to views and activating settings.	Configuring Permissions Navigation and Activate Settings on page 241
6	Configure user information	Configure User information including phone, e-mail, department and more.	Configuring User Information on page 242



Note: In addition to to the regular SecureSphere users, you can set permissions for the Active Directory users. For more information about integration with Active Directory, see **Configuring Integration with Active Directory** in the **SecureSphere User Guide**.

Working with Roles

Roles in SecureSphere reflect a role in your organization and contain a specific set of permissions required to perform that role. SecureSphere also contains a set of pre-defined roles which can be used.

Additionally, you can create new roles and customize them to match your company's workflow. The following subjects review various aspects of working with Roles:

- PreDefined Roles on page 234
- Creating a Role on page 235

PreDefined Roles

SecureSphere comes with a set of pre-defined roles to assist you in easily configuring users with the level of permissions required to fulfill their roles.



Note: Predefined roles cannot be modified.

The following is a list of these pre-defined roles and a short description of each:

Table 5 Pre-Defined Roles

Administrator	Main administrator user for SecureSphere. Assigned when first logging into SecureSphere. This user is responsible for managing SecureSphere and has permissions to all features and functionality.
Web/DB/File/SharePoint Security Admin	**Security Admins** are responsible for all the security aspects that deals with a specific product. For example, the Web Security Admin can create and edit services and applications, security policies and all global objects relevant to web products.
MX Admin	MX Admin role has View/Edit/Create permissions on all the MXs registered to that SOM and full visibility of all the policies and objects defined on SOM.

Custom Role Examples

The following are examples of custom roles that can be created to match a specific set of requirements.

Example 1: Managed Security Service Provider (MSSP)

MSSPs often offer third party solutions to their customers, and may want to provide some level of access to these products. In this case, you would want to provide view permissions to your customers for only those SecureSphere components that represent their specific services and applications, and provide navigation permissions under special permissions to the alerts screen. They would not obtain permissions to edit assets, policies, or global objects.

This can be done in different ways. For example, if you have 10 customers, each with only 1 user, you may want to create the user separately for each customer. Alternatively, you may want to create a role that would give navigation permissions to items such as monitoring, create individual users and include this role, then customize the user with permissions to view their specific assets.

Example 2: Web Services Engineer

If your organization utilizes a compartmentalized model such as a bank in which specific web services engineers should only have access to view details about specific services, you may want to:

- Create a new Role based the existing Web Security Admin
- Remove the Web Services and Applications that appear under Site Tree Object Type category
- Access each individual user, and under Web and Application Services (under site tree object types) click the edit button for these items, and select only those web services and applications you want the specific user to have access to.

Example 3: Audit Expert

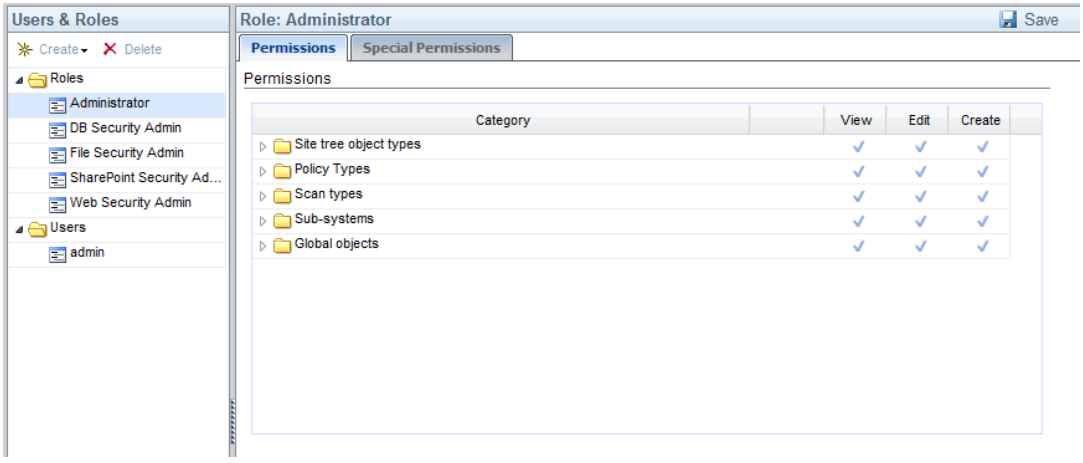
In some organizations there is a designated audit expert that creates audit policies, defines what data is audited, and how this data is handled. You may want to create a special Role for users who are responsible for creating these policies, but which prevent them from seeing actual audit data. In this case you could create a user (or role if there is more than one user with these responsibilities) which would only have create and edit permissions on audit policies. You may also want to provide them view permissions on a test database, which would enable them to test their policy as they are working on it, without exposing sensitive data.

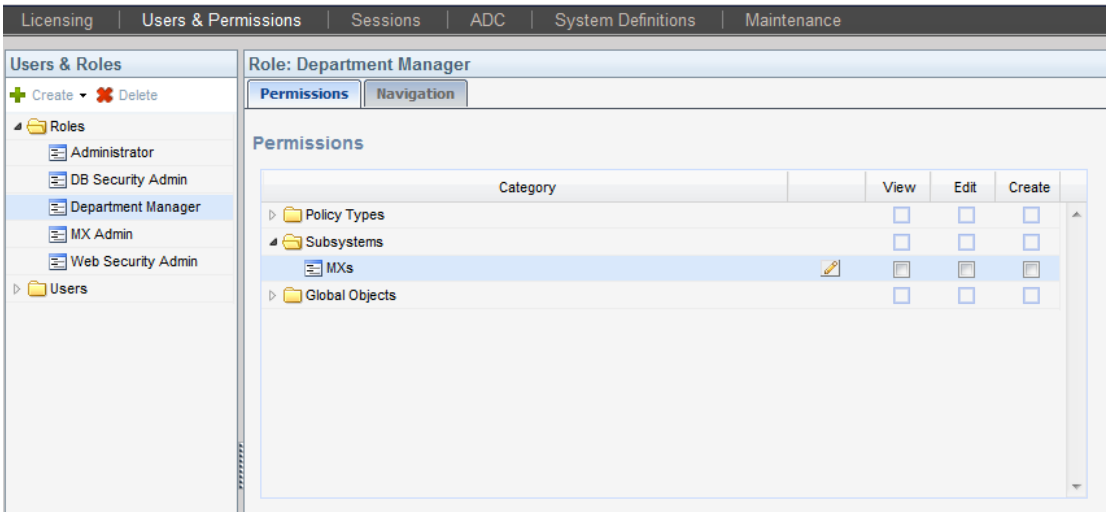
Creating a Role

SecureSphere comes with a number of pre-defined roles. You can additionally create custom roles to better match your company's environment.

To create a Role:

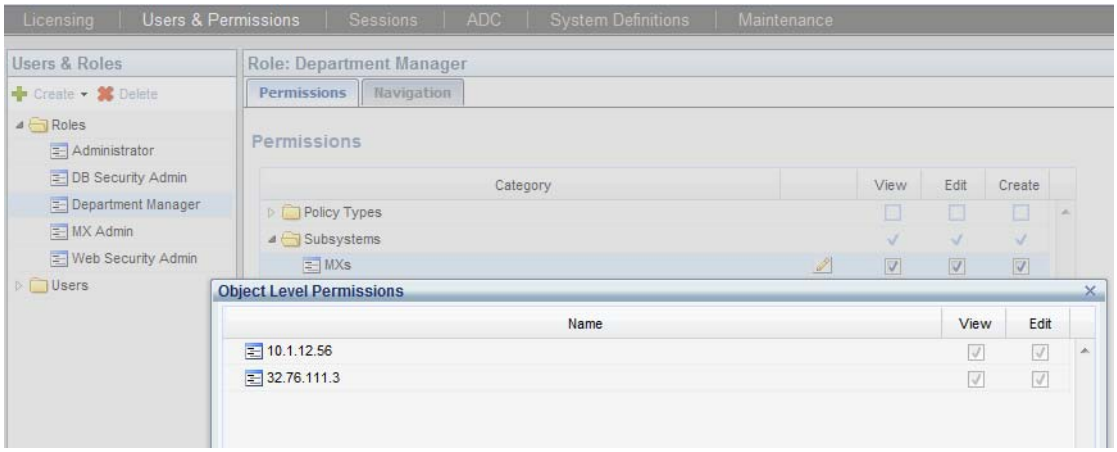
1. In the **Admin** workspace, select **Users and Permissions.**
2. In the **Users & Roles** pane, click , then **Create New Role**. The **Create New Role** window appears.
3. Type a **Name** for the role, then click **Create**. The new role is created and appears under **Roles** in the **Users and Roles** pane to the left-hand side of the window.





4. Configure this role with the desired permissions by selecting the role and defining permissions. When defining permissions in the **Permissions** pane, the same permissions are added to all the objects under that category.

5. To define different permissions for each object under the same category, click . The **Object Level Permissions** window appears.



6. Define the permissions that you want for each item in the **Object Level Permissions** list.

Working with Users

There are a number of aspects that are involved with working with users. They include the following:

- Creating a SecureSphere User on page 237
- Assigning Roles to Users on page 238
- Configuring Object or Category Level Permissions on page 238
- Configuring Permissions Navigation and Activate Settings on page 241
- Configuring User Information on page 242

Creating a SecureSphere User

Users in SecureSphere define a number of parameters that include roles to which a specific user is assigned, permissions to various SecureSphere objects ranging from site tree objects to global object, special permissions that provide access to views, and user information that define their full name, e-mail address, geographic location in the world, and more.

To create a SecureSphere User:

1. In the **Admin** workspace, select **Users and Permissions.**
2. In the **Users & Roles** pane, click , then **Create New User**. The Create New User window appears.
3. Type a **Name** for the user.
4. In **Authenticator**, select **SecureSphere** or **External** as appropriate.
   - **SecureSphere**: The user is authenticated by SecureSphere using a password (entered in **Password** below).
   - **External**: The user is authenticated using an external service, such as LDAP.

     In this case, the **Enter Password** and **Re-Enter Password fields** are ignored by SecureSphere, and the user is required to provide the password defined in the LDAP server.

     The user's name in SecureSphere must be identical to the user's CN in LDAP. Case sensitivity is enforced, that is, "Mary" is not identical to "mary".

     For information about configuring SecureSphere to work with LDAP, see External Systems - LDAP on page 313.
5. If **Authenticator** is **SecureSphere**, enter the user's password in **Enter Password** and again in **Re-Enter Password**.
6. If **Authenticator** is **LDAP**, you can lookup the user in the LDAP database by clicking **Lookup User**.

   If the in the **Authentication Configuration Window** is empty, then the test uses the user's SecureSphere password. Otherwise, you are prompted for the LDAP password.
7. Add one or more roles you want to assign the user by moving the desired roles to the Assigned pane. A role is a set of permissions to different objects. For more information on roles see Working with Roles on page 234
8. Click **Create**. The new user is created and appears under **Users** in the **Users and Roles** pane to the left-hand side of the window.

   You may now configure additional permissions for that user in addition to any permissions they are granted through roles. For more information see Configuring Object or Category Level Permissions on page 238.

Assigning Roles to Users

SecureSphere enables you to configure new users with roles and assign roles to existing users. By assigning roles to users you grant them the permissions that have been configured for the assigned roles.



Note: This procedure describes how to assign roles to existing users. Assigning roles to new users is part of the process of creating a new user. For information on assigning roles to new users, see Creating a SecureSphere User on page 237.

To assign a role to existing users:

1. In the **Admin** workspace, select **Users and Permissions.**
2. In the **Users & Roles** pane, expand the **Users** category, then select the user you want to assign a new role. That users details are displayed in the details pane.
3. On the permissions tab, move the role you want to assign the user from the **Selected** pane to the **Assigned** pane.

   Note: For information on creating new roles, see Creating a Role on page 235.
4. Click **Save**. Settings are saved and the user has now been granted the permissions available in the assigned role.

Configuring Object or Category Level Permissions

In addition to assigning users to a role, you have the option to assign them permissions to specific objects or categories of objects which may be relevant for their role or access model. For example, perhaps you are an ISP that provides SecureSphere as a paid service to your customers. And perhaps you'd like to give your customers only view access and only to their own web server. You could create a new user for each customer, and assign them additional (specific) view permissions for their web server.



Note: While you can add permissions on top of permissions provided through a predefined roles, you cannot revoke permissions that are part of these roles by default.

To configure additional permissions:

1. In the **Admin** workspace, select **Users and Permissions.**
2. In the **Users & Roles** pane, expand the **Users** category, then select the user you want to assign additional permissions. That users details are displayed in the details pane.
3. In the **Permissions** pane, navigate to the category and object you want to grant permissions to. For example, if you want to assign additional permissions to a specific policy, next to the policy category, click **Edit** .
4. Select the desired object level permissions. The item is selected, and the item representing permissions is displayed. For more information on how permissions are represented in the **Permissions** tab, see Understanding How Permissions are Displayed on page 239.
5. In the **Object Level Permissions** window click **Save**.
6. In the **Users and Roles** window from the upper right-hand corner of the screen. Click **Save**.
7. Your changes have been saved and the additional permissions have been assigned.

Understanding How Permissions are Displayed

The way that permissions are displayed for a user depends on what permissions have been configured on a specific object. Permissions have three possible levels as displayed in the permission window.

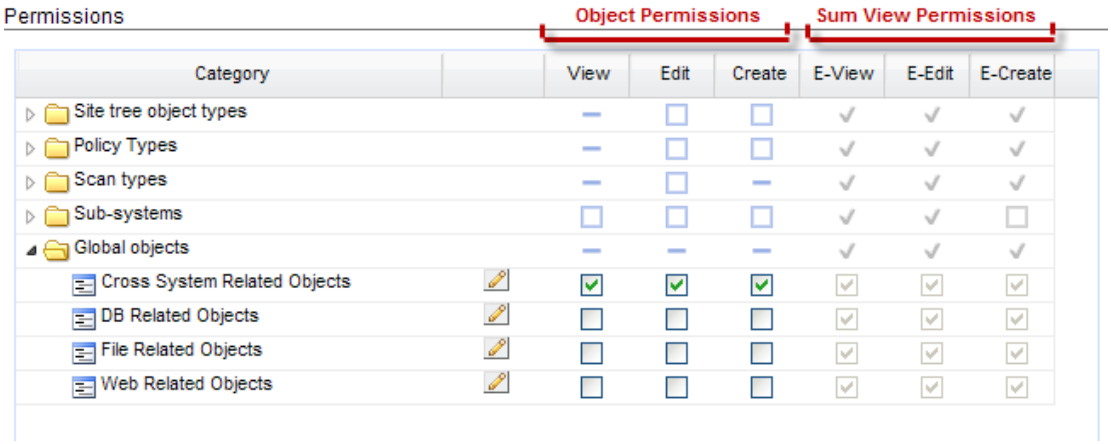
Table 6 Permission Levels

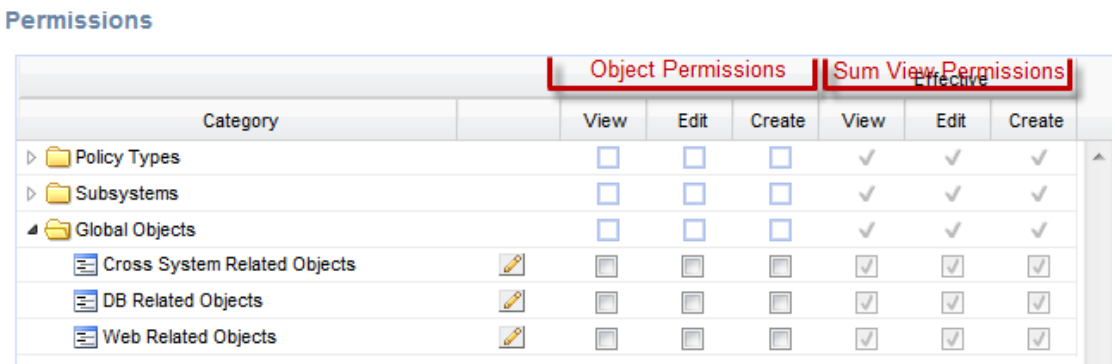
	Type	Description
☐	**None**	None of that category's object permissions have been assigned to the current user.
–	**Partial**	Some of the category's object permissions have been assigned to the current users.
✓	**Full**	All of the category's object permissions have been assigned to the current users.

Object View vs. Sum View

Permissions are displayed in SecureSphere on two levels:

- **Object View Permissions**: Displays permissions for the specific object only. For example, if a user has permissions to all Cross System Related Global objects as seen in the example below. Checkmarks are displayed for that category. Yet for the Global Objects category, you can see that hyphen symbols (partial) are displayed because this user does not have permissions to the other objects in that category.
- **Sum View Permissions**: Displays the sum of all permissions, both Object Level permissions, as well as permissions provided to users by roles they have been granted. So in the example below you can see that many of the objects the users have full permissions in Sum View, while under Object Permissions for the same items they only have partial permissions. This is due to the fact they have been granted additional permissions through their role which result in the user having all permissions for that object.





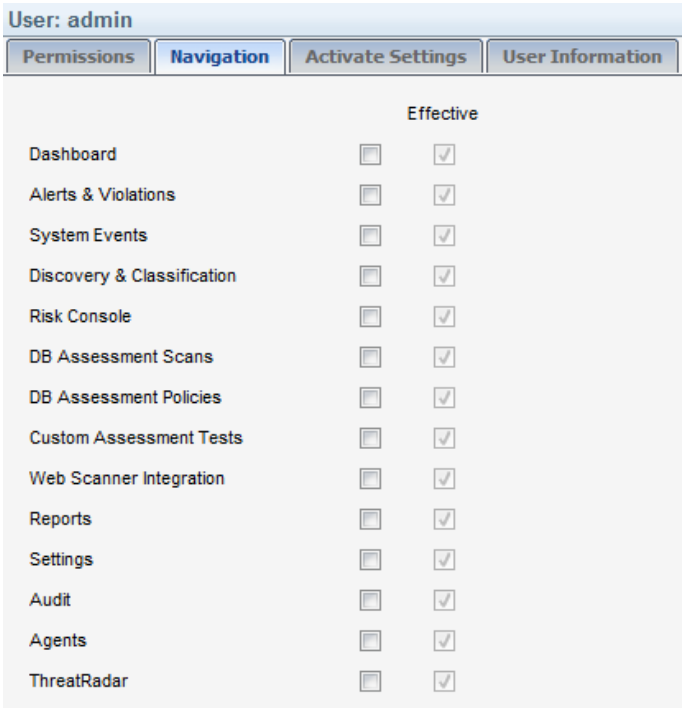
Configuring Permissions Navigation and Activate Settings

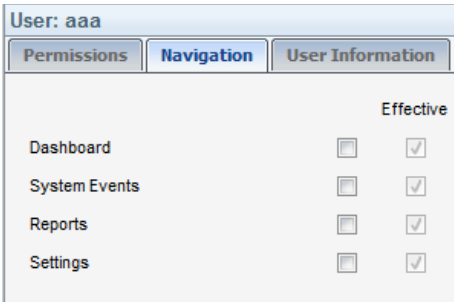
In the Navigation tab you can define permission to navigate to the enabled GUI windows.

Activate Settings defines under what conditions users can modify the SecureSphere database using the Activate Settings window.

To configure Navigation and Activate Settings:

1. In the **Admin** workspace, select **Users and Permissions.**
2. In the **Users & Roles** pane, expand the **Users** category, then select the user you want to assign navigation permissions. That users permissions are displayed in the details pane.
3. Click the **Navigation** tab. Navigation permission options are displayed.





4. To enable or disable permissions for any GUI window, select the appropriate options.



Note: An example of navigation permission might be that you want to allow a user to edit a certain database service but not see audit results. You would then give edit permissions on the service, but you wouldn't give navigation permissions on the audit screen.

5. In the **Activation Settings** tab select one of the following Activate Settings options:

Parameter	Description
The user is not authorized to perform Activate Settings.	The user does not have permission to use Activate Settings.
The user may only perform Activate Settings if authorized to view all changes that will be activated.	The user is allowed to perform Activate Settings only if he has permission to view all the parameters whose settings will be changed when Activate Settings is performed.
The user is authorized to perform Activate Settings unconditionally.	There are no restriction on the user in regard to the use of Activate Settings.

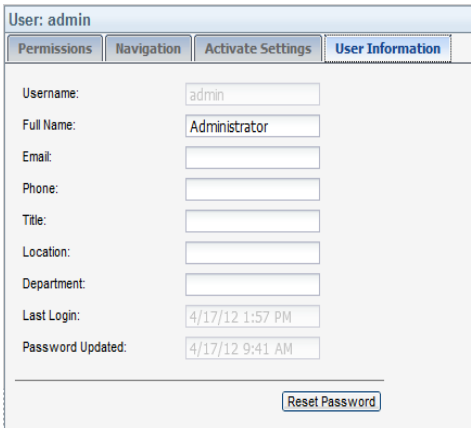
6. In the **Users and Roles** window from the upper right-hand corner of the screen. Click **Save**. Your settings have been saved.

Configuring User Information

When creating users it is recommended that you configure all the relevant details to identify that user. This can assist in communicating directly with a user, identifying to what department they belong, knowing their geographic location, and more.

To configure User Information:

1. In the **Admin** workspace, select **Users and Permissions.**
2. In the **Users & Roles** pane, expand the **Users** category, then select the user you whose information you want to edit. That users permissions are displayed in the details pane.
3. Click the **User Information** tab. User Information is displayed.



The **Username**, **Last login**, **Password Updated** fields are informative and cannot be changed in this window. You can enter data into the other fields without restriction.

Note: Enable or disable a user's account by selecting or deselecting **Account Enabled**. This field is useful for temporarily disabling a user without having to delete and later re-create the user.

CHAPTER 10

Sessions

This chapter describes the **Connected Users** window, which displays information about the users currently connected to the SecureSphere GUI, and includes the following:

Connected Users on page 245

Connected Users

The **Connected Users** pane displays information about the users currently connected to the SecureSphere GUI (that is, have open sessions).

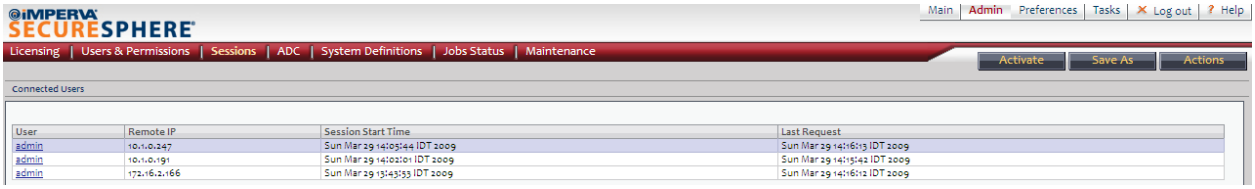


Figure 46 Sessions Window

For each user, the following information is displayed:

- **User**: The users name.
- **Remote IP**: The IP address from which the user is connected.
- **Session Start Time**: The date and time the session started.
- **Last Request**: The date and time of the last action performed by the user.

  The last action may be something as simple as displaying another tab in the GUI.

Sessions

Administrators can terminate (kill) sessions and disable users.

To kill a session:

1. In the **Admin** workspace, click **Sessions**.
2. In the **Connected Users** pane, select a user.
3. Click **Actions**.
4. From the menu, select **Kill User Session(s)**.

   All the user's sessions will be killed.



Note: An administrator cannot kill his own sessions or disable himself.

To disable a user and kill all of the user's sessions:

1. In the **Admin** workspace, click **Sessions**.
2. In the **Connected Users** pane, select a user.
3. Click **Actions**.
4. From the menu, select **Kill User Session(s) and Disable User**.

   All the user's sessions will be killed and the user will be logged off. The user will not be able to login again until he is enabled (see Working with Users on page 237).

CHAPTER 11

ADC

This chapter describes Imperva's Application Defence Center (ADC).

The Imperva Application Defense Center (ADC) is a premier research organization for security analysis, vulnerability discovery and compliance expertise. ADC research combines extensive lab work with hands-on testing in real world environments to ensure that Imperva's products, through advanced data security technology, deliver up-to-date threat protection and unparalleled compliance automation.

Having discovered dozens of commercial application vulnerabilities and having issued numerous security advisories, the ADC offers exceptional insight into both published and unpublished security threats.

ADC research not only provides an indispensable service to commercial application and database vendors and to security professionals, it also delivers the foundation for many Imperva SecureSphere features and services, including attack signature updates, database vulnerability assessments, and pre-defined compliance reports.

You can view and update ADC content, and view a history of ADC system events.

- Viewing ADC Content and Status on page 247
- Updating ADC Content on page 249
- ADC History on page 250

Viewing ADC Content and Status

To view the status of ADC updates:

1. In the **Admin** workspace, click **ADC**.

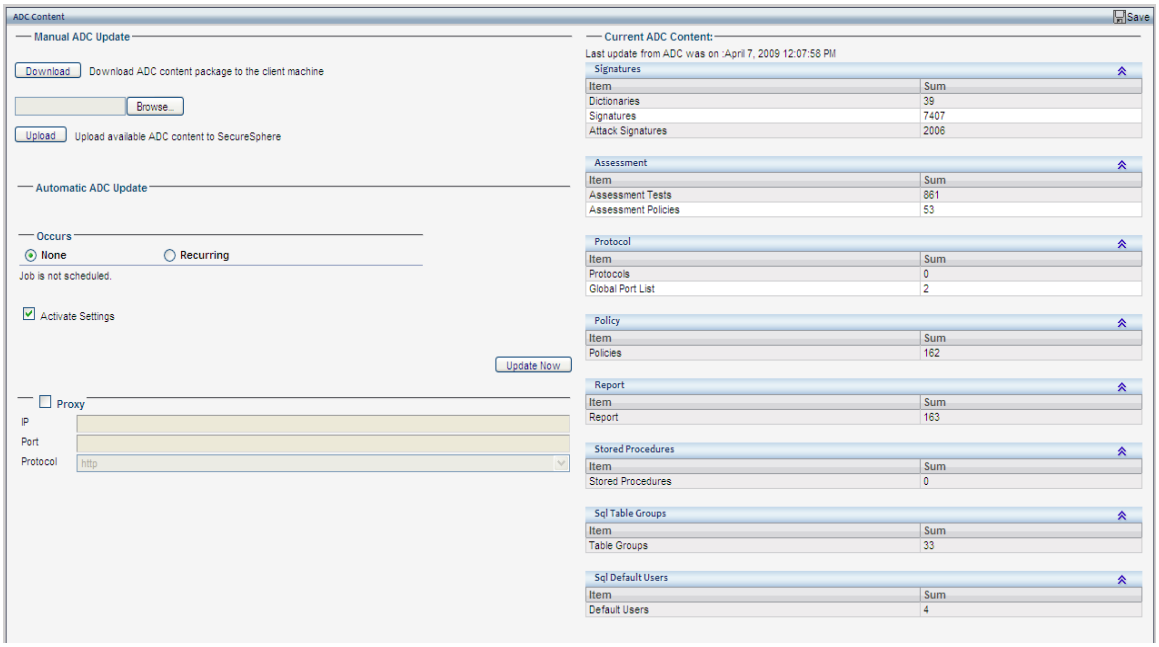


Figure 47 ADC Content window

2. In the **ADC Content** window, information about the ADC content last downloaded is displayed in the right half of the window, under **Current ADC Content**.

   The number of ADC Content items in each category is given under **Sum**.

   To hide the list of items in each category, click  (at the right end).

   To expand a hidden list, click .

   You can view the ADC content in the SecureSphere GUI, as listed below.

ADC content

Category	Item	Viewing the ADC Content for this category
Signatures	Dictionaries	In the **Main** workspace, select **Setup** > **Signatures**. The ADC dictionaries are listed under **Predefined Dictionaries** in the **Filter** pane.
	Signatures	In the **Main** workspace, select **Setup** > **Signatures**. Select a dictionary from those listed under **Predefined Dictionaries** in the **Filter** pane. The signatures belonging to the selected dictionary are displayed in the middle pane.
	Attack Signatures	

ADC content

Category	Item	Viewing the ADC Content for this category
Assessment	Assessment Policies	In the **Main** workspace, click **Risk Management** > **DB Assessment Policies**. Assessment Policies are displayed.
	Assessment Tests	In the **Main** workspace, click **Risk Management** > **DB Assessment Policies**. Then select a policy from the **Assessment Policies** pane. The tests belonging to that policy are displayed in the **Test List** tab of the rightmost pane.
Protocol	Protocols	
	Global Port List	In the **Main** workspace, select **Setup** > **Global Objects**. Under **Scope Selection**, select **Port Names**. **Note:** The number given under **Sum** for **Global Port List** is the number of lists, not the total number of ports in the lists.
Policy	Policies	The various ADC policies can be viewed in several different GUI locations. For example, to view the SAP-related ADC security policies, select **Main** > **Policies** and click **SAP** in the **Filter** pane (under **By ADC Keywords**). The SAP-related ADC security policies are displayed in the **Policies** pane.
Report	Report	In the **Main** workspace, select **Reports** > **Manage Reports** and, in the **Filter** pane, select **ADC** under **Defined By**.
Stored Procedures	Stored Procedures	In the **Main** workspace, select **Setup** > **Global Objects**. Under **Scope Selection**, select **DB Related Objects** > **Stored Procedure Groups** > **Built In**.
Sql Table Groups	Table Groups	In the **Main** workspace, select **Setup** > **Global Objects**. Under **Scope Selection**, select **DB Related Objects** > **Database Table Groups**.
Sql Default Users	Default Users	

Updating ADC Content

ADC content can be updated manually or automatically, on a scheduled basis.



Note: For information about using a proxy for ADC updates, see External HTTP Settings on page 306.

To manually update ADC content:

1. In the **Admin** workspace, click **ADC**.
2. Under **Manual ADC Update**, click **Download**.
3. Save the MPRV file that will be downloaded.
4. Browse to the downloaded file using the **Browse** button.
5. Click **Upload**.

   SecureSphere will be updated with the downloaded content.



Note: Some of the updates will not take effect until you Apply Settings.

To schedule automatic updating of ADC content:

1. In the **Admin** workspace, click **ADC**.
2. Under **Manual ADC Update**, select **Recurring**.
3. Define the schedule for automatic ADC updates.
4. To specify that Activate Settings be performed immediately after a successful automatic update of ADC content, select **Activate Settings**.
5. To update ADC content immediately, click **Update Now**.



Note: For ADC update to succeed, the Default Gateway and the DNS server must be set using `impcfg`.

ADC History

To view the history of ADC-related events:

1. In the **Main** workspace, click **Monitor** > **System Events**.
2. In the **Filter** pane, under **By SubSystem**, select **ADC**.

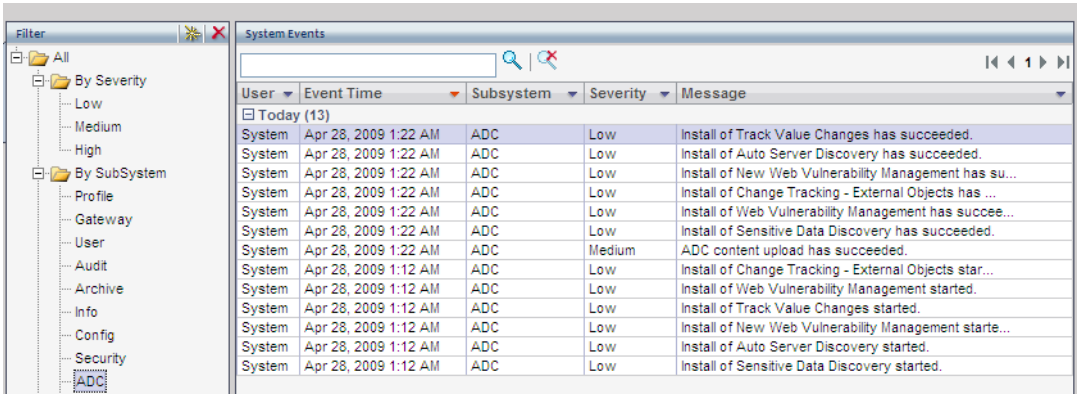


Figure 48 ADC History

CHAPTER 12

Job Status

This chapter describes the **Jobs Status** window, and includes the following:

Jobs Status on page 253

Jobs Status

The **Jobs Status** window displays information about jobs which were run or are currently running.

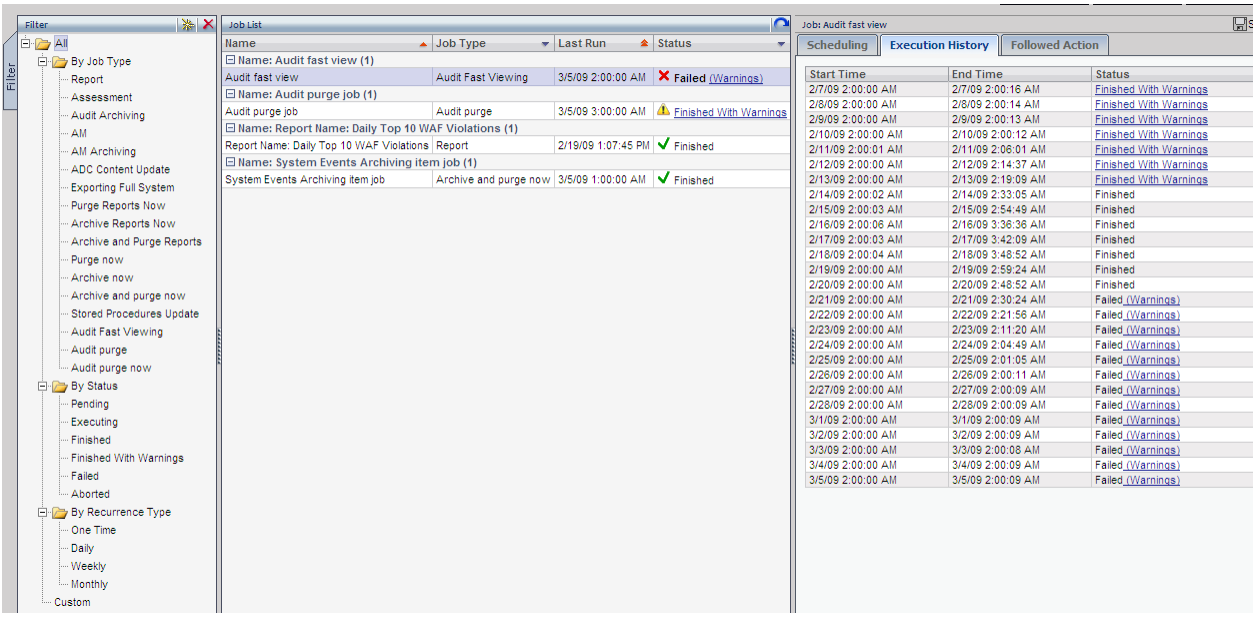


Figure 49 Job List Window

For each job, the following information is displayed:

- **Name**: The job's name.
- **Job Type**: The job's type.
- **Last Run**: The date and time the job was last executed.
- **Status**: The status of the job's last execution. If the job's status is not "Finished", you can click on the status to display an explanation of the status.
- **Next Run**: The date and time of the next scheduled run.

  The  icon indicates that the job is recurring. Hover the mouse over the icon to display the schedule.

In the rightmost pane, there are three tabs which display information about the job currently selected in the **Job List** pane:

- **Scheduling**: This tab displays the schedule for running the job.
- **Execution History**: A chronologically-ordered list of all executions of the job, with the last execution at the bottom of the list.
- **Followed Action**: This tab displays the job's followed action.

Displaying the Jobs Status Window

To display the Jobs Status window:

1. In the **Admin** workspace, click **Jobs Status**.
2. In the **Filter** pane, you can define a filter on the jobs to be displayed in the **Job List** pane.
3. In the **Job List** pane, the last execution of jobs which have already run are displayed. You can refresh the list by clicking  in the upper-right corner of the **Job List** pane.

Editing a Job

You cannot change jobs which have already run, or have already started running, but you can change the scheduling and Followed Actions for future executions of a job.

To change a job's scheduling:

1. In the **Admin** workspace, click **Jobs Status**.
2. In the **Filter** pane, you can define a filter on the jobs to be displayed in the **Job List** pane.
3. In the **Job List** pane, select a job.
4. Click the **Scheduling** tab.
5. Under **Occurs**, select one of the following:

Parameter	Description
None	The job is never run.
One Time	The job is run on the date and time you specify in **At** and **At Time**.
Recurring	The job is run periodically according to the schedule you define.

6. Click **Save**.

To change a job's followed action:

1. In the **Admin** workspace, click **Jobs Status**.
2. In the **Filter** pane, you can define a filter on the jobs to be displayed in the **Job List** pane.
3. In the **Job List** pane, select a job.
4. Click the **Followed Action** tab.
5. Select a **Followed Action**.
   For information on creating followed actions, see ***SecureSphere User Guide***.
6. Click **Save**.

Aborting a Job

To abort a currently running job:

1. In the **Admin** workspace, click **Jobs Status**.
2. In the **Filter** pane, you can define a filter on the jobs to be displayed in the **Job List** pane.
3. In the **Job List** pane, right-click a job and select **Abort** from the menu.
   If **Abort** is greyed-out, the job has already finished running and cannot be aborted.

CHAPTER 13

Maintenance

This chapter describes various system maintenance tasks, and includes:

Audit Fast Viewing on page 256
Audit Purge on page 257
Assessment Results Archive on page 258
Discovery Results Archive on page 260
Exporting and Importing the Management Server on page 262
Reports Archive on page 269
Risk Score Update on page 270
Kerberos Key Update on page 271
System Events Archive on page 272
Vulnerabilities Purge on page 274
Extracting Archives for Viewing on page 275
Audit Archive Conversion on page 276

Audit Fast Viewing

The **Audit Fast Viewing** window specifies the parameters for retrieving audit data for audit policies.

To define the parameters for audit fast view:

1. In the **Admin** workspace, click **Maintenance**.
2. In the **Maintenance** pane, click **Audit Fast Viewing**.

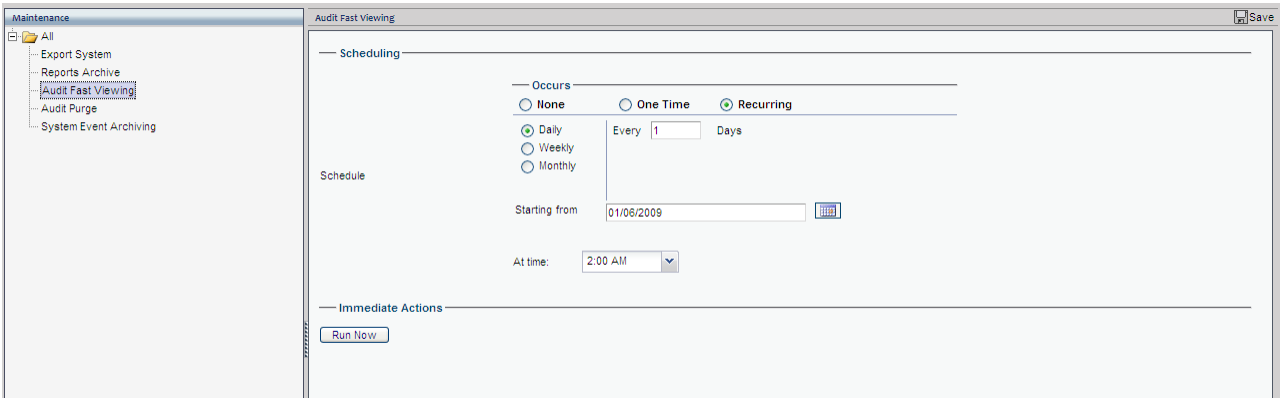


Figure 50 System Maintenance - Audit Fast Viewing

3. In the **Scheduling** section, under **Occurs**, select one of the following:

Parameter	Description
None	Audit data are not retrieved automatically. If this option is selected, the only way to retrieve audit data are to do so manually, by clicking **Run Now**.
Once	Audit data are retrieved automatically on the date and time you specify in **At** and **At Time**.
Recurring	Audit data are retrieved automatically according to the schedule you define.

4. Click **Run Now** to retrieve audit data immediately.



Note: The number of days of audit data retrieved in defined individually for each audit policy.

5. Click **Save**.

Audit Purge

The **Audit Purge** window specifies the parameters for purging audit data for all gateways being managed by SecureSphere.

To configure audit purge per audit policy, you need to configure **archiving** for Audit policies. For more information on configuring audit policies, see the ***SecureSphere User Guide***.

To define the parameters for purging audit data:

1. In the **Admin** workspace, click **Maintenance**.
2. In the **Maintenance** pane, click **Audit Purge**.

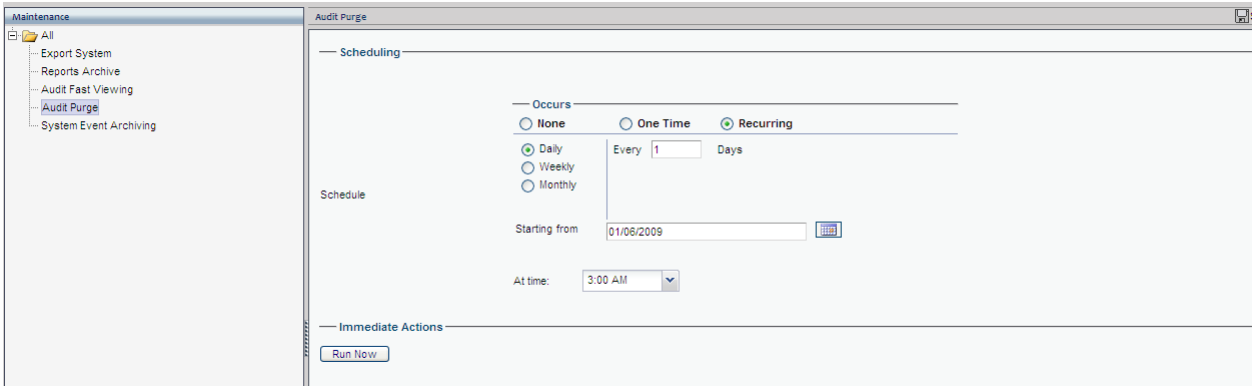


Figure 51 System Maintenance - Audit Purge

3. In the **Scheduling** section, under **Occurs**, select one of the following:

Parameter	Description
None	Audit data are not purged automatically. If this option is selected, the only way to retrieve purge data is to do so manually, by clicking **Run Now**.
Once	Audit data are purged automatically on the date and time you specify in **At** and **At Time**.
Recurring	Audit data are purged automatically according to the schedule you define.

4. Click **Run Now** to purge audit data immediately.

   Before purging, make sure the audit data have been successfully archived.
5. Click **Save**.

Assessment Results Archive

The **Assessment Results Archive** window specifies the parameters for archiving assessment results.

To define the parameters for archiving of Assessment results:

1. In the **Admin** workspace, click **Maintenance**.
2. In the **Maintenance** pane, click **Assessment Results Archive.**

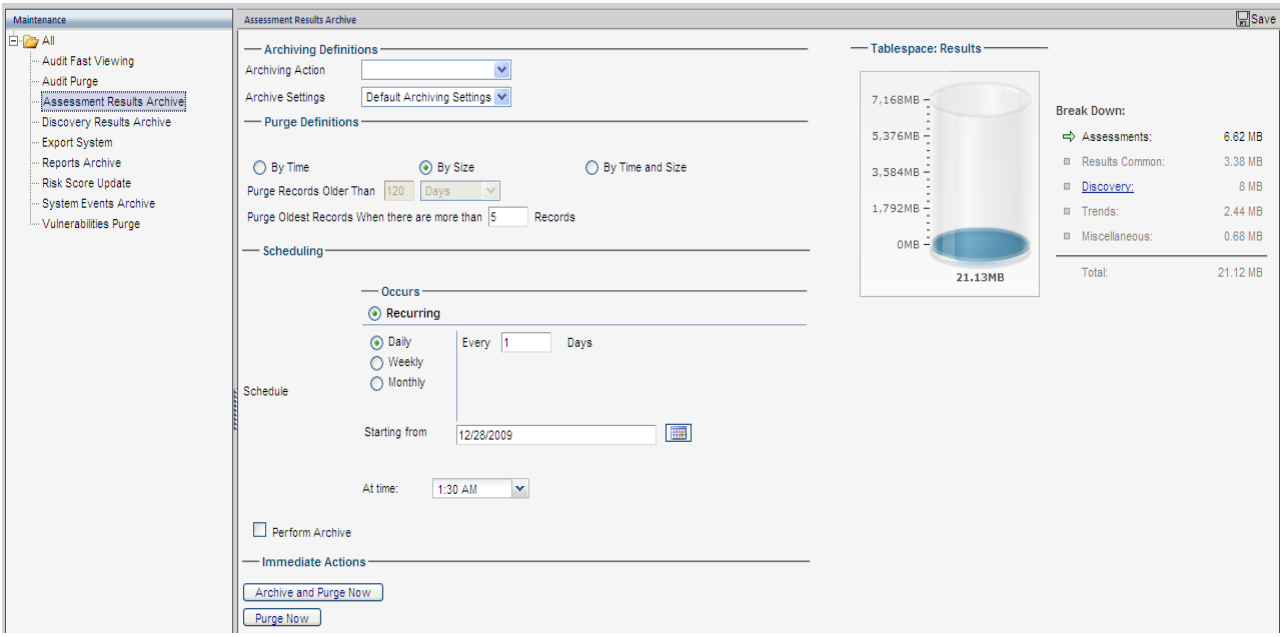


Figure 52 System Maintenance - Assessment Results Archive

3. In the **Archiving Definitions** section, set the following parameters:

Parameter	Description
Archiving Action	From the menu, select the Action Set to be performed after archiving assessment results.
Archive Settings	From the menu, select the archive settings.



Note: The Archive Setting menu item **Default Archive Settings** does not by default encrypt the archive file. To change these settings, in the **Main** workspace, select **Setup** > **Settings** and then select **Archive Settings** from the **Settings** pane, select **Default Archive Settings** and enter the encryption keys. Alternatively, you can define another archive setting in **Main** > **Setup** > **Settings** and use it here.

4. In the **Purge Definitions** section, select one of the following:

Parameter	Description
By Time - Purge Records Older Than	Purge results older than the specified age.
By Size - Purge Oldest Records When there are more than Than ... Records	When the number of results exceeds the specified number, purge the oldest records.



Note: The default is **By Size - Purge Oldest Records When there are more than Than 100,000 Records**, meaning that by default, no more than 100,000 results are available.

5. In the **Scheduling** section, under **Occurs**, select one of the following:

Parameter	Description
None	Results data are not purged automatically. If this option is selected, the only way to purge results data is to do so manually, by clicking **Run Now**.
Once	Results data are purged automatically on the date and time you specify in **At** and **At Time**.
Recurring	Results data are purged automatically according to the schedule you define.

6. Select **Perform Archive** to archive the data before purging.
7. Click **Archive and Purge Now** to archive the data immediately then purge it from SecureSphere.
8. Click **Purge Now** to purge results data immediately.
9. Click **Save**. For information on how to extract assessment or discovery result archives for viewing in its source format, see Extracting Archives for Viewing on page 275.

Managing System Events

Discovery Results Archive

The **Discovery Results Archive** window specifies the parameters for archiving assessment results.

To define the parameters for archiving of Discovery results:

1. In the **Admin** workspace, click **Maintenance**.
2. In the **Maintenance** pane, click **Discovery Results Archive.**

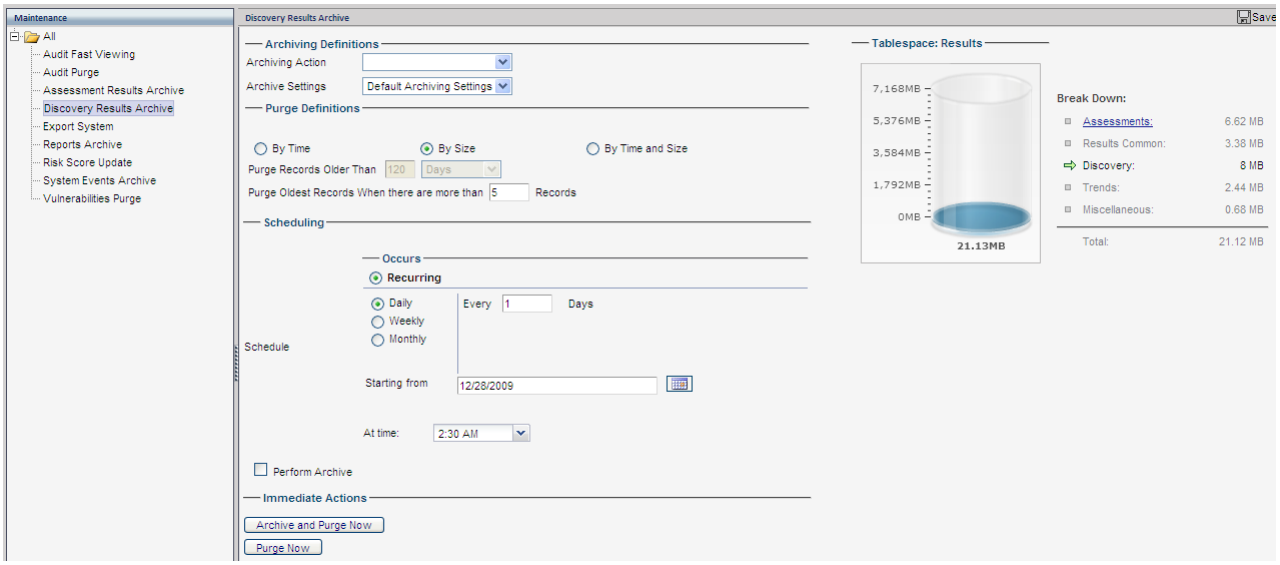


Figure 53 System Maintenance - Discovery Results Archive

3. In the **Archiving Definitions** section, set the following parameters:

Parameter	Description
Archiving Action	From the menu, select the Action Set to be performed after archiving assessment results.
Archive Settings	From the menu, select the archive settings.



Note: The Archive Setting menu item **Default Archive Settings** does not by default encrypt the archive file. To change these settings, in the **Main** workspace, select **Setup** > **Settings** and then select **Archive Settings** from the **Settings** pane, select **Default Archive Settings** and enter the encryption keys. Alternatively, you can define another archive setting in **Main** > **Setup** > **Settings** and use it here.

4. In the **Purge Definitions** section, select one of the following:

Parameter	Description
By Time - Purge Records Older Than	Purge results older than the specified age.
By Size - Purge Oldest Records When there are more than Than ... Records	When the number of results exceeds the specified number, purge the oldest records.



Note: The default is **By Size - Purge Oldest Records When there are more than Than 100,000 Records**, meaning that by default, no more than 100,000 results are available.

5. In the **Scheduling** section, under **Occurs**, select one of the following:

Parameter	Description
None	Results data are not purged automatically. If this option is selected, the only way to purge results data is to do so manually, by clicking **Run Now**.
One Time	Results data are purged automatically on the date and time you specify in **At** and **At Time**.
Recurring	Results data are purged automatically according to the schedule you define.

6. Select **Perform Archive** to archive the data before purging.
7. Click **Archive and Purge Now** to archive the data immediately then purge it from SecureSphere.
8. Click **Purge Now** to purge results data immediately.
9. Click **Save**. For information on how to extract assessment or discovery result archives for viewing in its source format, see Extracting Archives for Viewing on page 275.

Exporting and Importing the Management Server

You can export and import the SecureSphere data from the Management Server, including configuration files, the SecureSphere database, and (optionally) alerts data. Any data that arrives at the Management Server after the export operation begins is not included in the export file.

Exporting and importing are useful for the following purposes:

- copying a database to another machine
- backing up a database

You can perform these functions in any of the following ways:

- export using the management interface
- import and/or export using the interactive command line interface (CLI)
- import and/or export using the non-interactive command line interface (CLI)

Note: You cannot use the SecureSphere GUI to import a SecureSphere database, because you must stop the SecureSphere Management Server during the import process.

Export Using the SecureSphere GUI

To export a SecureSphere database:

1. In the **Admin** workspace, click **Maintenance**.
2. In the **Maintenance** pane, click **Export System**.

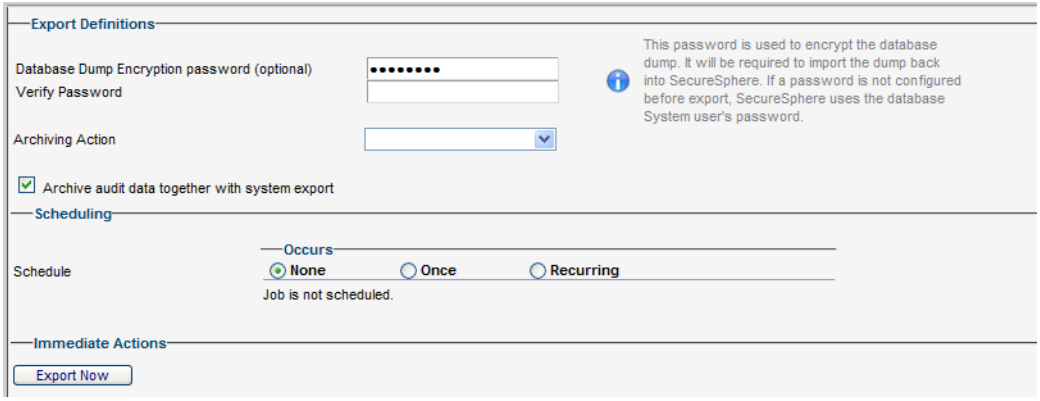


Figure 54 System Maintenance - Export System

3. In the **Export Settings** pane, in the **Export Definition** section, enter the following data.

Parameter	Description
Database Dump Encryption Password	The dump file is always encrypted. You can use the system password (the password of the DBA of the SecureSphere database) or specify another password. To specify another password, enter the password in **Database Dump Encryption Password** and re-enter the same password in **Verify Password.** If you do not enter an encryption password, the export file will be encrypted with the system password (the password of the DBA of the SecureSphere database). **Note:** You will not be able to import the encrypted dump file without the password. There is no workaround.
Verify Password	

Archiving Action	Select an Action Set from the dropdown list.
	Note: By default, only the **Default Archive Action Set** is available. To use a different Action Set:
	1. Define an Action Interface of type NFS Archive (**Admin** > **System Definitions** > **Action Interfaces**).
	2. Define an Action Set of type **Archiving** which uses the Action Interface you defined in the previous step (**Main** > **Policies** > **Action Sets**).
	3. In the Action Interface's **Destination Directory**, specify the **Destination Directory** for the archive.
	4. If the destination directory is not the default directory (`/var/tmp`), then you must also ensure that SecureSphere has the required permissions in that directory by executing the following OS commands:
	`chmod 777`
	`chown mxserver:mxserver`
	Select the Action Set you have just configured for **Archiving Action**.

4. In the **Scheduling** section, under **Occurs**, select one of the following:

Parameter	Description
None	The export is never scheduled, but you can run it at any time by clicking **Export Now**.
One Time	The export is run on the date and time you specify in **At** and **At Time**.
Recurring	The export is run periodically according to the schedule you define.

5. Click **Save**.
6. Alternatively, you can perform the export immediately by clicking **Export Now**.

The name of the export file is of the form: `/tmp/SecureSphere_<date>.dmp.gz`, where `<date>` is the current date in the format YYYYMMDD.

Export / Import Manually Using the Interactive CLI



Note: There are at least four users defined on a Management Server:
- root: the OS superuser
- secure: a SecureSphere CLI user, with access only to `impcfg`
- system: the DBA of the SecureSphere database
- admin: a SecureSphere administrator with access to the SecureSphere GUI; any number of SecureSphere administrators and users can be defined



Note: Do not export while the ADC database is being updated, otherwise the exported file will be corrupted.

To export SecureSphere data using the interactive CLI:

1. Login to the SecureSphere Management Server as `root`.
2. Execute the following command:

```
full_expimp.sh
```

3. Enter the following data when requested:
   - **operation**: Select `1` (export).
   - **system password**: Enter the system password (the password of the DBA of the SecureSphere database).
   - **export type**: Select `1` to export the alert data as well.
   - **export failed archive files:** Select `y` to include failed archive data (default is not to export).
   - **encryption password**: Enter a password for encrypting the dump file (the default is system password, that is, the password of the DBA of the SecureSphere database).
   - **export file**: Enter the name of the export file. The full name of the export file will be `<file_name>.dmp.gz`, where `<file_name>` is the name you enter here.
4. Enter `Y` to confirm the export.

To import SecureSphere data using the interactive CLI:

1. Login to the SecureSphere Management Server as `root`.
2. Stop the SecureSphere Management Server by executing the following command:

   ```
   impctl server stop
   ```
3. Execute the following command:

   ```
   full_expimp.sh
   ```
4. Enter the following data when requested:
   - **operation**: Select `2` (import).
   - **system password**: Enter the system password (the password of the DBA of the SecureSphere database).
   - **import type**: Select `1` to drop the target schema, that is, before starting the import operation, delete the schema on the machine to which the export file is being imported.

     This is the recommended option, since it ensures that the resulting data will consist only of the imported data.
   - **copy option**: Select 1 to copy the configuration files, that is, files not part of the SecureSphere database, for example:
     `SecureSphereWork/firsttime/firsttimeIds`,
     `SecureSphereWork/firsttime/mutableFirsttimeIds`,
     `SecureSphereWork/activated-configuration`

- **secure password**: The password of the SecureSphere CLI user.
- **import file**: Enter the fullpath name of the import file, that is, the previously exported file.

5. You will be asked whether the file is encrypted. If you answer `Y` (the default), then you will be asked to enter the encryption password.
6. Enter `Y` to confirm the import.
7. Start the SecureSphere Management Server by executing the following command:

   ```
   impctl server start
   ```

8. Review the import log for errors or warnings.

Listing the Contents of an Exported File

To list the contents of an exported file:

1. Login to the SecureSphere Management Server as `root`.
2. Execute the following command:

   ```
   full_expimp.sh
   ```

3. Enter the following data when requested:
   - **operation**: Select `3` (List dump file content).
   - **encryption password**: If the file is encrypted, enter a passwordthe password (the default password is system password, that is, the password of the DBA of the SecureSphere database).
   - **Enter a file name for the operation**: Enter the fullpath name of a previously-exported file.
4. The output will be similar to the following:

```
full_expimp (version 2.0) started on Sun May  3 15:02:56 IDT 2009

Decompressing dump file
Dump file contains the following schemas:
SECURE
SECURE_DA

Dump contains SecureSphere version: 7.0.0.7014.Release
Dump was created using full_expimp version: 2.0

full_expimp completed successfully on Sun May  3 15:02:57 IDT 2009
```

Export / Import Manually Using the Non-Interactive CLI

You can export and/or import the SecureSphere data using the `full_expimp.sh` command while specifying the options in the command line.

To export SecureSphere data using the non-interactive CLI:



Note: Do not export while the ADC database is being updated, otherwise the exported file will be corrupted.

1. Login to the SecureSphere Management Server as **root**.
2. Execute the following command, adding some or all the additional parameters listed in the following table:

```
full_expimp.sh --operation=1 --pwd=<password> --copyfiles=<copy_option>   --
logfile=<file_name>" --schema=<schema>
```



Note:
- The exported file is always encrypted. The default password is the system password, that is, the password of the DBA of the SecureSphere database), although you can specify a different password using the **pwd** argument.
- The table below lists only the most frequently used import and export options. For a complete list of these options, enter the following command:
  full_expimp.sh ?

full_expimp.sh Export Parameters

Parameter	Description
--dmpfile=<file>	The destination file for the exported data. If not specified, the default is **/tmp/SecureSphere_<date>** where **<date>** is the current date in the format YYYYMMDD.
--exptype=<n>	Specifies whether the export will include alert data: • 1 - include the alert data • 2 - do not include alert data **default**: 1
--schema=<name>	Export only the **<name>** schema from the database. If not specified, the script will export the following database schemas: • SECURE • SECURE_DA • all ODM schemas
--copyfiles=<copy_option>	Specify 1 to copy the configuration files, that is, files not part of the SecureSphere database, for example: • **SecureSphereWork/firsttime/firsttimeIds**, **SecureSphereWork/firsttime/mutableFirsttimeIds**, **SecureSphereWork/activated-configuration**
--logfile=<file_name>	Specifies the location of the log file.



Note: The SecureSphere database comprises the following schemas:
- SECURE: The SecureSphere configuration and data
- SECURE_DA: Changes made to the SecureSphere configuration which have not yet been applied
- ODM: Active Module schemas

To import SecureSphere data using the non-interactive CLI:

1. Login to the SecureSphere Management Server as **root**.
2. Execute the following command, adding some or all the additional parameters listed in the following table:

```
full_expimp.sh --operation=2 --pwd=<password> --dmpfile=<file>
```



Note:
- The exported file is always encrypted. The default password is the system password, that is, the password of the DBA of the SecureSphere database), although you can specify a different password using the **pwd** argument.
- The table below lists only the most frequently used import and export options. For a complete list of these options, enter the following command:
  full_expimp.sh ?

full_expimp.sh Import Parameters

Parameter	Description
--imptype=<n>	Specifies whether the import will first delete imported schemas from the database: • 1 - delete imported schemas from the database • 2 - do not delete imported schemas from the database **default**: 1 If you specify 1 (delete imported schemas), then if the import file includes only one schema, only that schema is deleted from the database. If the import file includes all schemas, the following database schemas are deleted from the database: • SECURE • SECURE_DA • all ODM schemas
--copyfiles=<n>	Specifies whether to import configuration files (files not part of the SecureSphere database), for example: **SecureSphereWork/firsttime/firsttimeIds**, **SecureSphereWork/firsttime/mutableFirsttimeIds**, **SecureSphereWork/activated-configuration**. • 1 - import configuration files • 2 - do not import configuration files
--src=<name>	Specify this parameter to import only the **<name>** schema from the exported file.
--dest=<name>	If you have specified the **--src** parameter, the **--dest** parameter enables you to rename the imported schema in the target database. For example, if the exported file contains the SECURE schema, you can import it to SECURE_OLD by specifying: **--src=secure --dest=secure_old**
--tbsname=<name>	Import all the imported objects to the **<name>** tablespace instead of the tablespace they were in the source database.
--tbsloc=<path>	This option is set if you want to import the entire data of the imported objects to a specific tablespace instead of the tablespaces they were in the source database.

Miscellaneous Maintenance Tasks

To list the contents of an exported file:

1. Login to the SecureSphere Management Server as **root**.
2. Execute the following command:
   full_expimp.sh --operation=3 --dmpfile=<file>



Note: If you import a system setup that was exported from a Onebox appliance to a different Onebox appliance, delete the Gateway from **Setup** > **Gateways** and then re-register the Gateway.

Reports Archive

The **Reports Archive** window specifies the parameters for archiving reports.

To define the parameters for archiving reports:

1. In the **Admin** workspace, click **Maintenance**.
2. In the **Maintenance** pane, click **Reports Archive.**

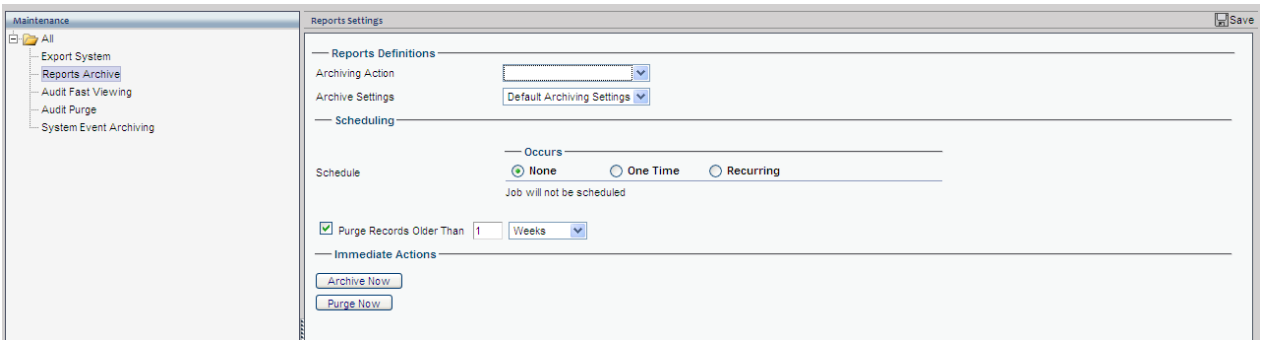


Figure 55 System Maintenance - Reports Archive

3. In the **Reports Definition** section, set the following parameters:

Parameter	Description
Archiving Action	From the menu, select the Action Set to be performed after archiving reports.
Archive Settings	From the menu, select the archive settings.

Note: The Archive Setting menu item Default Archive Settings does not by default encrypt the archive file. To change these settings, in the Main workspace, select Setup > Settings and then select Archive Settings from the Settings pane, select Default Archive Settings and enter the encryption keys. Alternatively, you can define another archive setting in Main > Setup > Settings and use it here.

4. In the **Scheduling** section, under **Occurs**, select one of the following:

Parameter	Description
None	Reports are not archived automatically. If this option is selected, the only way to archive reports is to do so manually, by clicking **Archive Now**.
One Time	Reports are archived automatically on the date and time you specify in **At** and **At Time**.
Recurring	Reports are archived automatically according to the schedule you define.

5. Click **Archive Now** to archive reports.
6. Click **Purge Now** to purge report data.

   Before purging, make sure the reports have been successfully archived.
7. Click **Save**. Report archiving has been configured. For information on how to extract report archives for viewing in its source format, see Extracting Archives for Viewing on page 275.

Risk Score Update

You can change the frequency of the risk score update.

To change the schedule of the risk score update:

1. In the **Admin** workspace, click **Maintenance**.
2. In the **Maintenance** pane, click **Risk Score Update**.

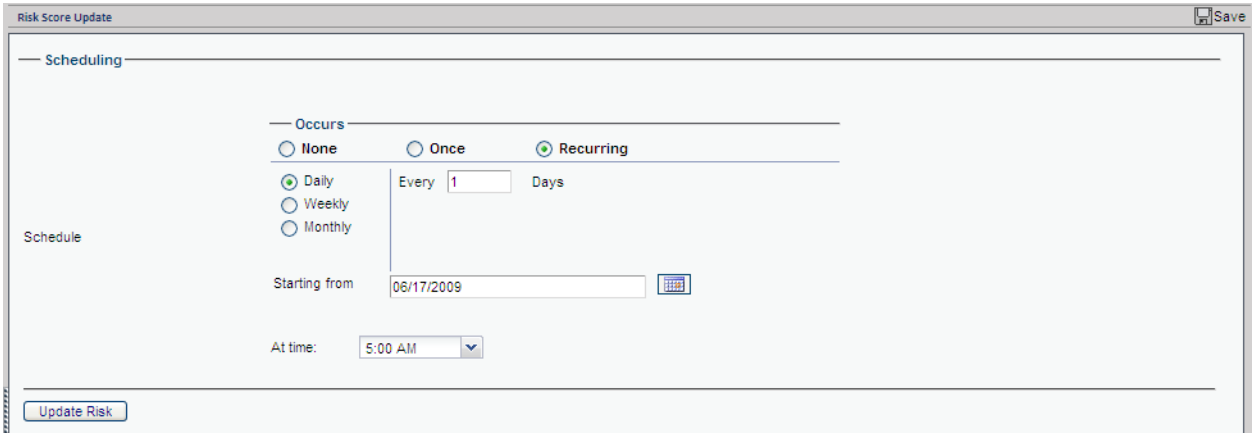


Figure 56 System Maintenance - Risk Score Update

3. In the **Scheduling** pane, under **Occurs**, select one of the following:

Parameter	Description
None	The risk score update is never scheduled, but you can update it at any time by clicking **Update Now**.
One Time	The risk score is updated on the date and time you specify in **At** and **At Time**.
Recurring	The risk score is updated periodically according to the schedule you define.

4. Click **Save**.
5. To update the risk score immediateluy, click **Update Now**.

Kerberos Key Update

The **Kerberos Key Update** window specifies the parameters for updating Kerberos keys.

To define the parameters for updating Kerberos keys:

1. In the **Admin** workspace, click **Maintenance**.
2. In the **Maintenance** pane, click **Kerberos Key Update.**

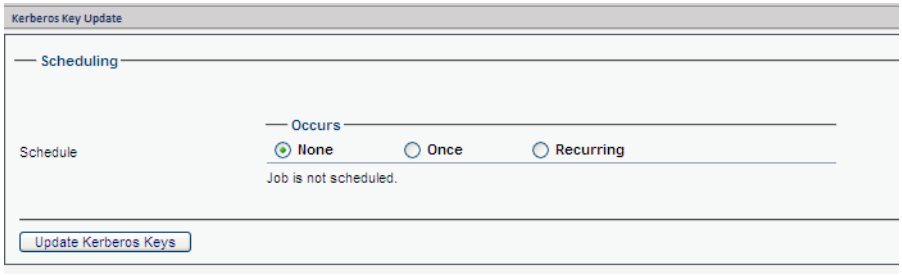


Figure 57 System Maintenance - Kerberos Key Update

3. In the **Scheduling** section, under **Occurs**, select one of the following:

Parameter	Description
None	Kerberos keys are not updated automatically. If this option is selected, the only way to Kerberos keys is to do so manually, by clicking **Run Now**.
One Time	Kerberos keys are updated automatically on the date and time you specify in **At** and **At Time**.
Recurring	Kerberos keys are updated automatically according to the schedule you define.

4. Click **Update Kerberos Keys** to update all Kerberos keys immediately.

System Events Archive

The **System Event Archive** window specifies the parameters for archiving system event data.

To define the parameters for archiving system event data:

1. In the **Admin** workspace, click **Maintenance**.
2. In the **Maintenance** pane, click **System Events Archive.**

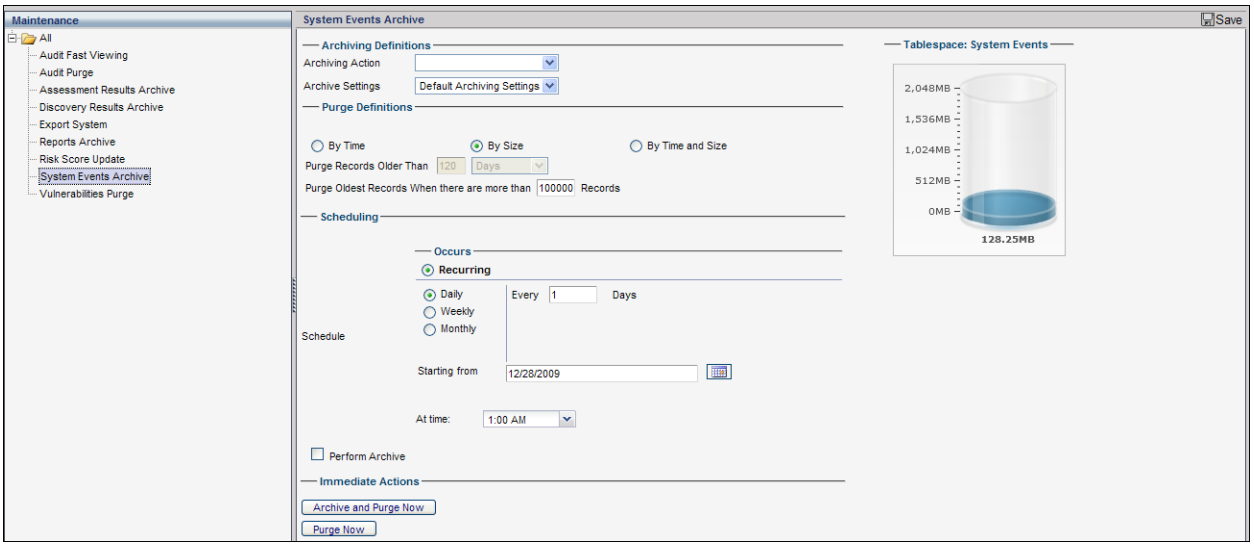


Figure 58 System Maintenance - System Events Archive

3. In the **Archiving Definitions** section, set the following parameters:

Parameter	Description
Archiving Action	From the menu, select the Action Set to be performed after archiving system events.
Archive Settings	From the menu, select the archive settings.



Note: The Archive Setting menu item Default Archive Settings does not by default encrypt the archive file. To change these settings, in the Main workspace, select Setup > Settings and then select Archive Settings from the Settings pane, select Default Archive Settings and enter the encryption keys. Alternatively, you can define another archive setting in Main > Setup > Settings and use it here.

4. In the **Purge Definitions** section, select one of the following:

Parameter	Description
By Time - Purge Records Older Than	Purge system events older than the specified age.
By Size - Purge Oldest Records When there are more than Than ... Records	When the number of system events exceeds the specified number, purge the oldest records.



Note: The default is **By Size - Purge Oldest Records When there are more than Than 100,000 Records**, meaning that by default, no more than 100,000 system events are available.

5. In the **Scheduling** section, under **Occurs**, select one of the following:

Parameter	Description
None	System event data are not purged automatically. If this option is selected, the only way to purge system event data is to do so manually, by clicking **Run Now**.
One Time	System event data are purged automatically on the date and time you specify in **At** and **At Time**.
Recurring	System event data are purged automatically according to the schedule you define.

6. Select **Perform Archive** to archive the system event data before purging.
7. Click **Archive and Purge Now** to archive the data immediately then purge it from SecureSphere.
8. Click **Purge Now** to purge the system event data immediately.
9. Click **Save**. For information on how to extract system event archives for viewing in its source format, see Extracting Archives for Viewing on page 275.

Vulnerabilities Purge

The **Vulnerabilities Purge** window specifies the parameters for purging vulnerability data for all gateways being managed by SecureSphere.

To define the parameters for purging vulnerability data:

1. In the **Admin** workspace, click **Maintenance**.
2. In the **Maintenance** pane, click **Vulnerability Purge**.

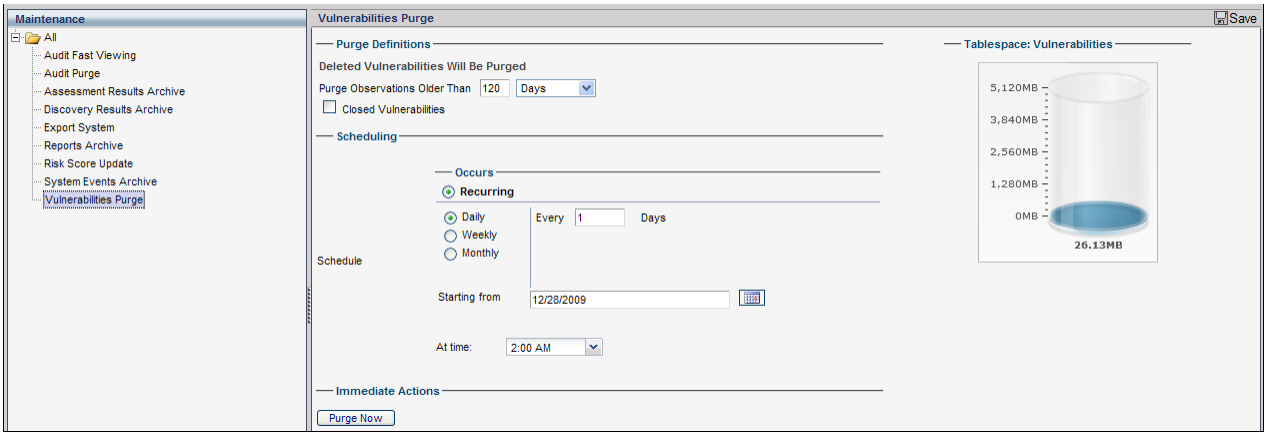


Figure 59 System Maintenance - Audit Purge

3. In the Purge Definitions section, configure the following:

Parameter	Description
Purge Observations Older Than	Determines the period of time for which vulerabilities should be purged from SecureSphere. You can enter a number, then a timeperiod that includes days, months weeks and months. For example, you can configure SecureSphere to purge vulnerabilities that have been observed for the past 12 weeks.
Closed Vulnerabilities	When selected, purges all vulnerabilities in the SecureSphere server that have been closed.

4. In the **Scheduling** section, under **Occurs**, select one of the following:

Parameter	Description
None	Audit data are not purged automatically. If this option is selected, the only way to retrieve purge data is to do so manually, by clicking **Run Now**.
One Time	Audit data are purged automatically on the date and time you specify in **At** and **At Time**.
Recurring	Audit data are purged automatically according to the schedule you define.

5. Click **Run Now** to purge audit data immediately.
   Before purging, make sure the audit data have been successfully archived.
6. Click **Save**.

Extracting Archives for Viewing

While information that has been archived from SecureSphere cannot be imported back into SecureSphere, it can be extracted and viewed in its source format. This includes the following:

- Reports
- System Events
- Assessment Results
- Discovery Results

To extract and view data that have previously been exported from SecureSphere:

1. Copy the archive file to the SecureSphere server under the `\tmp` directory.
2. Run the following command:

```
java -jar ~mxserver/bin/packagertool.jar -unpack -target <target_dir> -
source <source_mprv_file> -keystore <server_kst_file>
-encAlias <encryption_alias> -sigAlias <signature_alias>
```

where

- **source**: The script's source can be either an mprv file to unpack, or a directory of audit files to pack back to an mprv file.
- **target**: The script's target can be either an mprv file to pack to, or a directory of to unpack the mprv file to.
- **keystore**: The new version keystore file. On the Server, the file is located at:
  `/opt/SecureSphere/server/SecureSphere/jakarta-tomcat-secsph/conf/securesphere.kst`
- **newEncAlias**: New encryption key alias (optional)
- **newSigAlias**: New signature alias (optional)
- **encKey**: Old version encryption private key pem file (optional: use if archive is encrypted)
- **encPass**: Old version encryption password (optional: use if archive is encrypted)
- **sigKey**: Old version signature private key pem file (optional: use if archive is signed)
- **sigPass**: Old version encryption password (optional: use if archive is signed)

3. Copy file(s) indicated in the message to your desktop, and rename by adding the extension `.tar`.
4. Extract the contents of the file. The reports contained in the archive are now available for viewing in original (PDF/CSV) format.



Notes:
- To use sigAlias and encAlias on management server, list the key's name without its path.
- Key names can be taken from **Setup** > **Archive Settings**.



Note: To repack the CSV files back to an MPRV file, execute:
java -jar ~mxserver\bin\packagertool.jar -pack -target <target_mprv_file> -source <source_dir> -keystore <server_kst_file> -encAlias <encryption_alias> -sigAlias <signature_alias>

EXAMPLE: EXTRACTING A FILE FOR VIEWING

java -jar ~mxserver/bin/packagertool.jar -unpack -target /tmp -source /tmp/archive-reports_20100502-141103_-9031273315142595961.mprv -keystore /opt/SecureSphere/server/SecureSphere/jakarta-tomcat-secsph/conf/securesphere.kst

Audit Archive Conversion

Audit archives can be converted using an action interface to CSV format, which can then be opened and analyzed with external tools such as those used for business intelligence. This section provides instructions on how to use the audit export tool to convert archives previously exported in standard SecureSphere MPRV format versions 6.2 and up. Both of these processes convert archives into CSV format packaged in a single TAR file.

The following procedures for converting and analyzing audit archives are available:

- Exporting an Archive to TAR Format with CSV Values on page 276
- Converting an MPRV file to TAR Format with CSV Values on page 277
- Analyzing Converted Files on page 277

Exporting an Archive to TAR Format with CSV Values

This procedure describes how to configure a SecureSphere Run a Shell Command action interface to export audit files to CSV format and package them in a TAR file. Audit files then archived using this action interface can later be imported into a business intelligence tool and analyzed.

To configure a Run a Shell Command action interface for converting archive data:

1. Create directories in which to store both the unconverted mprv files and the converted CSV files, and change the owner of the directories to **mxserver**, by executing the following commands, substituting your own directory names:

```
mkdir <mprv files directory> <csv files directory>
chown mxserver <mprv files directory> <csv files directory>
```

2. In the SecureSphere **Main** workspace, select **Policies > Action Sets**. The **Action Sets** window appears.
3. In the **Action Sets** pane, click **New**. The **Action Set** dialog box appears.
4. Enter a name for the action set.
5. In the **Apply to** event type drop-down menu, select **Archiving**, then click **OK**. An action set is created.
6. Click the green arrow of the **OS Command** > **Run a Shell Command** action interface. The action interface is moved up to the **Selected Actions** pane.
7. Expand the action interface and configure its parameters as follows:

Parameter	Description
Name	Enter a name for the action interface.
Command	`/opt/SecureSphere/server/bin/processArchive.sh`

Arguments	`${Job.file} [OriginalArchiveLocation] [SCPtargetlocation] [OptionalEncryptionAlias] [OptionalSigningAlias]`
	Example:
	`${Job.file} root@10.1.1.21:/tmp/ root@10.1.1.21:/tmp/`
	See below for an explanation of the arguments.

Working Dir	`/opt/SecureSphere/server/bin`

Argument	Description
${Job.file}	A placeholder that indicates the location of the original archive.
[OriginalArchiveLocation]	The SCP location to which the **unconverted** archive should be copied. **Note:** This directory must already exist, and the owner must be set to "mxserver".
[SCPtargetlocation]	The SCP location to which the **converted** archive should be copied. **Note:** This directory must already exist and the owner must be set to "mxserver".
[OptionalEncryptionAlias]	Encryption alias, as used in the Archive Settings (optional)
[OptionalSigningAlias]	Signing alias, as used in the Archive Settings (optional)

8. From the upper right-hand corner of the screen, click **Save**.

   When audit information is archived using this action interface, they will be packaged as CSV files in a TAR file and saved to the locations you configured in the arguments of the script.

   The log of the script is written to `/var/tmp/archive-convert-full.log and /var/tmp/archive-convert-error.log`

   Due to file size/archiving limits, a single TAR file from a single audit policy may contain multiple, similar values. Special care must be taken to guarantee that it contains only unique values. In order to achieve this you should perform a "select distinct".

   In case one of the files cannot be copied to the target location, it will be written to `/var/tmp/failed_delivery`
9. You should periodically delete the un-needed mprv and the TAR'ed CSV files to free disk space.

Converting an MPRV file to TAR Format with CSV Values

This procedure describes how to use the audit archive tool to repackage MPRV archives previously exported using SecureSphere 6.2 and newer. This process processes binary information added as part of advanced audit archive creation and produces a TAR file containing audit data in CSV format.

To convert MPRV files 6.2 and newer to TAR with CSV:

1. Copy the archives you want to convert to the SecureSphere host.
2. Run the following commands on the desired files using the Command Line.



Note: If the archive is encrypted or signed, you will need to use the relevant keys.

- chmod +x ./convertAuditFiles.sh
- ./convertAuditFiles.sh

The files are converted to CSV and packaged into TAR format.



Note: Due to file size/archiving limits, a single TAR file from a single audit policy may contain multiple, similar values. Special care must be taken to guarantee it only contains unique values. In order to achieve this you should conduct a "select distinct".

Analyzing Converted Files

Once you have converted your audit archive files to CSV format, you can load them into the desired tool for analysis and run queries as desired.

To analyze converted files:

1. Load the CSV output from the extracted archives into your database.
   - In order to do so, you should understand the format of data and tables that are required. For more information, see Data Format on page 278.
   - For an illustration of the relationship between tables see Relationship between Tables on page 280.
2. Run queries as required to match your needs, if required use join between the index and events. For a list of sample queries, see Sample Queries on page 280.

Data Format

This section reviews the types of information that are included in the audit archive (SecureSphere 6.2 and newer), after being converted to CSV files using the conversion tool. Use this information to load the CSV files into an external database and create appropriate links between the tables.



Note: When loading results into a non-Oracle database, an equivalent type should be used. For example VARCHAR2(4000 BYTE) should be some kind of string column of at least 4000 bytes. NUMBER(19,0) should be numeric column that supports numbers of 19 digits (decimal), etc.

1. **#.events CSV: table name in SecureSphere - AUDIT_EVENTS.**

   This file includes the following columns and their types (specified as a Oracle type):

   RESPONSE_INFO" VARCHAR2(4000 BYTE),
   "EVENT_ID" NUMBER(19,0),
   "EVENT_CREATION_TIME" DATE,
   "DEBUG_INFO" VARCHAR2(4000 BYTE),
   "STREAM_ID" NUMBER(19,0),
   "SOURCE_PORT" NUMBER(19,0),
   "DESTINATION_PORT" NUMBER(19,0),
   "ORIGINAL_USER_NAME" VARCHAR2(4000 BYTE),
   "RAW_QUERY" VARCHAR2(4000 BYTE),
   "PARSED_QUERY" VARCHAR2(4000 BYTE),
   "BIND_VARS" VARCHAR2(4000 BYTE),
   "URL" VARCHAR2(4000 BYTE),
   "SESSION_ID" NUMBER(19,0),
   "WEB_EVENT_ID" NUMBER(19,0),
   "WEB_SOURCE_IP" VARCHAR2(16 BYTE),
   "EXCEPTION_STRING" VARCHAR2(4000 BYTE),
   "RESPONSE_SIZE" NUMBER(19,0),
   "RESPONSE_TIME" NUMBER(19,0),
   "AFFECTED_ROWS" NUMBER(19,0),
   "AGENT" VARCHAR2(4000 BYTE),
   "LOG_COLLECTOR_NAME" VARCHAR2(4000 BYTE),
   "REAL_DATE_TIME" DATE,
   "QUERY_GROUP" VARCHAR2(4000 BYTE),
   "REPORT_COUNT" NUMBER(19,0),
   "TICKET_ID" VARCHAR2(4000 BYTE),
   "CUSTOM_TAGS" VARCHAR2(4000 BYTE)



Notes:

- 6.2 vs. 7.0 Columns: The last 2 columns are available only in 7.0.
- Delimiter: The CSV file always includes an extra column (last) with value END. This can be used as a line delimiter ("END\n") for loaders which don't support newline characters inside data.

2. **Index (AKA Keys) - #.crc2key.csv, table name in SecureSphere - AUDIT_KEYS:**
   Includes the following:
   "CRC" NUMBER(19,0),
   "SERVER_GROUP_LC_ID" NUMBER(19,0),
   "SERVICE_LC_ID" NUMBER(19,0),
   "APPLICATION_LC_ID" NUMBER(19,0),
   "EVENT_SOURCE_TYPE" VARCHAR2(20 BYTE),
   "USER_TYPE" VARCHAR2(20 BYTE),
   "DB_USER" VARCHAR2(100 BYTE),
   "SQL_SOURCE_GROUP" VARCHAR2(4000 BYTE),
   "USER_AUTHENTICATED" NUMBER(1,0),
   "APPLICATION_USER_NAME" VARCHAR2(4000 BYTE),
   "SOURCE_IP" VARCHAR2(16 BYTE),
   "SOURCE_APP" VARCHAR2(4000 BYTE),
   "OS_USER" VARCHAR2(4000 BYTE),
   "HOST" VARCHAR2(4000 BYTE),
   "SERVICE_TYPE" VARCHAR2(20 BYTE),
   "DESTINATION_IP" VARCHAR2(16 BYTE),
   "EVENT_TYPE" VARCHAR2(20 BYTE),
   "OPERATION" VARCHAR2(4000 BYTE),
   "OPERATION_TYPE" VARCHAR2(4000 BYTE),
   "OPERATION_OBJECT" VARCHAR2(4000 BYTE),
   "OPERATION_OBJECT_TYPE" VARCHAR2(4000 BYTE),
   "SUBJECT" VARCHAR2(4000 BYTE),
   "DATABASE" VARCHAR2(4000 BYTE),
   "SCHEMA" VARCHAR2(4000 BYTE),
   "TABLE_GROUP" VARCHAR2(4000 BYTE),
   "SENSITIVE" NUMBER(1,0),
   "PRIVILEGED" NUMBER(1,0),
   "STORED_PROCEDURE" NUMBER(1,0),
   "EXCEPTION_OCCURRED" NUMBER(1,0),
   "QUERY_CRC" NUMBER(19,0),
   "RESPONSE_SIZE" VARCHAR2(20 BYTE),
   "AFFECTED_ROWS" VARCHAR2(20 BYTE),
   "RESPONSE_TIME_BUCKET" VARCHAR2(20 BYTE),
   "USER_DEFINED_TAG_1" VARCHAR2(4000 BYTE),
   "USER_DEFINED_TAG_2" VARCHAR2(4000 BYTE),
   "IS_TICKET" NUMBER(1,0),



Notes:

- 6.2 vs. 7.0 Columns: The last 3 columns are available only in 7.0.
- Delimiter: The CSV file always includes an extra column (last) with value END. This can be used as a line delimiter ("END\n") for loaders which don't support newline characters inside data.
- Server Group / Service / Application: These columns include item ids and not names.

3. **Index to Events Mapping - #.crc2event.csv, table name in SecureSphere - AUDIT_EVENT_TO_KEY:**

   Includes the following:

   "EVENT_ID" NUMBER(19,0),

   "CRC" NUMBER(19,0),

4. **Responses - #.responses.csv, table name in SecureSphere - AUDIT_RESPONSES:**

   Includes the following:

   "EVENT_ID" NUMBER(19,0),

   "RESULT_SET_INDEX" NUMBER(10,0),

   "ROW_INDEX" NUMBER(19,0),

   "COL1" VARCHAR2(4000 BYTE),

   "COL2" VARCHAR2(4000 BYTE),

   "COL3" VARCHAR2(4000 BYTE),

Relationship between Tables

The above tables can be joined in order to query data based on both indexes and events for example, or on events and responses:

- Events table AUDIT_EVENTS column "EVENT_ID" and mapping table AUDIT_EVENT_TO_KEY column "EVENT_ID"
- Index table AUDIT_KEYS column "CRC" and mapping table AUDIT_EVENT_TO_KEY column "CRC"
- Events table AUDIT_EVENTS column "EVENT_ID" and responses table AUDIT_RESPONSES column "EVENT_ID".

Sample Queries

This section lists a number of examples to illustrate the different types of queries that can be used to extract information based on the type of information you wish to extract. The examples below work with the latest versions of Oracle and MS-SQL databases, but may not be compatible with other DB types or with older Oracle/MS-SQL versions.

In all examples below:

- Results include distinct rows (no duplicates).
- When events is accessed, duplicate event ids (EVENT_ID) are ignored by selecting the row with the highest REPORT_COUNT value.

Example 1 (Index Only)

1. Get list of users (DB_USER), and tables/operations that they accessed (OPERATION_OBJECT / OPERATION), sort by user.

```
select distinct
    db_user,
    operation_object,
    operation
from audit_keys
order by db_user;
```

2. Get list of tables/operations that specific user "my_user" accessed (filter), sort by table.

```
select distinct
    operation_object,
    operation
from audit_keys
where db_user='MY_USER'
order by operation_object;
```

3. Get list of users and for each distinct count of the parsed queries (QUERY_CRC) that the user executed, sorted by count.

```
select
    db_user,
    count(distinct query_crc)
from audit_keys
group by db_user
order by count(distinct query_crc) desc;
```

Example 2 (Index + Events)

1. Get list of users and distinct parsed queries (PARSED_QUERY), sorted by user.

```
select distinct
    audit_keys.db_user,
    audit_events.parsed_query
from
    audit_keys,
    audit_events,
    audit_event_to_key
where
    audit_event_to_key.crc=audit_keys.crc and
    audit_event_to_key.event_id=audit_events.event_id
order by db_user;
```

2. Get list of tables filtered by specific user "my_user", for each the sum of the following:

```
RESPONSE_SIZE / RESPONSE_TIME / AFFECTED_ROWS. Sorted by table name.
select
    audit_keys.operation_object,
    sum(audit_events.response_size),
    sum(audit_events.response_time),
    sum(audit_events.affected_rows)
from
    audit_keys,
    (select response_size,response_time,affected_rows,event_id,row_number()
over (partition by event_id order by report_count desc) relevant from
audit_events) audit_events,
    audit_event_to_key
where
    audit_events.relevant=1 and
    audit_event_to_key.crc=audit_keys.crc and
    audit_event_to_key.event_id=audit_events.event_id and
    audit_keys.db_user='MY_USER'
group by audit_keys.operation_object
order by operation_object;
```

3. Get list of users and full list raw queries (RAW_QUERY) that they executed, with event id (EVENT_ID) and time stamp (EVENT_CREATION_TIME).

```
select distinct
    audit_keys.db_user,
    audit_events.raw_query,
    audit_events.event_id,
    audit_events.event_creation_time
from
    audit_keys,
    (select raw_query,event_creation_time,event_id,row_number() over
(partition by event_id order by report_count desc) relevant from
audit_events) audit_events,
    audit_event_to_key
where
    audit_events.relevant=1 and
    audit_event_to_key.crc=audit_keys.crc and
    audit_event_to_key.event_id=audit_events.event_id
order by db_user;
```

Example 3 (Index + Events + Responses)

1. Get all responses (data) that specific user "my_user" retrieved from specific tables "my_table_1" or "my_table_2". This is done by finding events ids matching the filter, then getting all rows from the responses table with this event id.

```
select
    *
from
    audit_responses
where
    event_id in (select audit_events.event_id
                 from audit_keys,
                      audit_events,
                      audit_event_to_key
                 where
                      audit_event_to_key.crc=audit_keys.crc and
                      audit_event_to_key.event_id=audit_events.event_id and
                      audit_keys.db_user='MY_USER' and
                      operation_object in ('MY_TABLE_1','MY_TABLE_2')
                );
```

CHAPTER 14

System Definitions

This chapter describes the parameters defined under **System Definitions** in the **Admin** workspace, and includes:

Dynamic Profiling on page 287
- Learning Exceptions on page 287
- Profile Optimization on page 287
- Profile Size Limits on page 288
- Switching to Protect Mode Thresholds (SQL) on page 291
- Switching to Protect Mode Thresholds (Web) on page 294

Gateway Settings on page 295
- Audit Settings on page 296
- Response Page Display in Alerts Settings on page 296
- Web to Database User Tracking Settings on page 296

Security and Authentication on page 298
- Authentication and Authorization Configuration on page 298
- FIPS Settings on page 298
- Password Settings on page 299
- SSL Certificate Expiration Monitoring on page 300

Management Server Settings on page 301
- Action Interfaces on page 301
- Agents on page 303
- Alert Aggregation Configuration on page 304
- Application Groups Settings on page 305
- Assessments on page 305
- CSV Upload Default Settings on page 305

Data Owner Settings on page 306
External HTTP Settings on page 306
External Systems on page 307
External Systems - Active Directory Collection (Forest) on page 309
External Systems - Kerberos Authentication on page 310
External Systems - LDAP on page 313
External System - LDAP Authentication and Authorization on page 313
External System - RADIUS Authentication on page 315
External System - SQL on page 316
External System - SSH Proxy on page 316
File URM on page 317
Keywords Settings on page 317
Log Collectors on page 319
Lookup Data on page 320
Policy Settings on page 321
Report Settings on page 321
Server Definitions on page 322
Stored Procedures Settings on page 322
System Events Notifications on page 323
User Interface Settings on page 325
Display Limits on page 325
Language Settings on page 325
ThreatRadar Settings on page 326
General Settings on page 326

Dynamic Profiling

This section describes the windows related to profiling, and includes:

Learning Exceptions on page 287
Profile Optimization on page 287
Profile Size Limits on page 288
Switching to Protect Mode Thresholds (SQL) on page 291
Switching to Protect Mode Thresholds (Web) on page 294

Learning Exceptions

These parameters define exceptions to the Web profile learning process.

If you change any of these parameters, click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the ***SecureSphere User Guide***.

Learning Exceptions Window Parameters

Parameter	Description
Don't learn requests that have no referer, unless the response code appears in this list:	As a rule, HTTP requests with no referer information are not learned, unless the target URL was already observed at least once. However, if the request's response codes appears in this comma-separated list, the request will be learned. Specify “none” to indicate no exclusions. **Default**: 200, 304
Don't learn requests with an unknown external host, unless the response code appears in this list:	As a rule, if an HTTP request has a host name which was not yet learned, and the request’s referer is external (that is, it does not appear in the list of learned hosts), the request will not be learned. However, if the request's response codes is this comma-separated list, the request will be learned. Specify “none” to indicate no exclusions. **Default**: 200, 304

Profile Optimization

These parameters define exceptions to the profile optimization process.

If you change any of these parameters, click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the ***SecureSphere User Guide***.

Profile Optimization Window Parameters

Parameter	Description
Alert Occurrences	The number of times alerts need to take place within **Alert Timeframe in Hours** to generate an optimization issue.
Alert Timeframe in Hours	The period of time in which the number of alerts need to occur to generate an optimization issue.
Size Limit (%)	The percentage of the Profile Size Limit (see Profile Size Limits on page 288) which, when reached, generates an optimization issue.

Profile Size Limits

When one of these limits is exceeded, SecureSphere stops learning the application and issues a profile size violation system event.

You should not increase any of these values unless there is a compelling reason to believe that the limits will be exceeded, because a profile's size can impact both Gateway and MX performance. If you find yourself regularly exceeding these limits, then you should attempt to address the issue by using URL patterns, plugins or other methods before concluding that the limits must be increased.

The following table lists the parameters in the **Profile Size Limit** pane.

If you change any of these parameters, click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the ***SecureSphere User Guide***.

Profile Size Limits Window Parameters

Parameter	Description
Maximum allowed source applications per user	For DB profiles, the maximum number of applications allowed in a user's profile. When this number is exceeded, no additional applications are added to the relevant profile and a warning message is written to the system log. If the profile reaches this limit, consider allowing any application for the relevant user. **Default**: 1000
Maximum allowed databases per user	For DB profiles, the maximum number of databases allowed in a user's profile. When this number is exceeded, no additional databases are added to the relevant profile and a warning message is written to the system log. If the profile reaches this limit, consider allowing any database for the relevant user. **Default**: 1000
Maximum allowed source host names per user	For DB profiles, the maximum number of source host names allowed in a user's profile. When SecureSphere reaches this number, no additional host names are added to the relevant profile and a warning message is written to the system log. If the profile reaches this limit, consider allowing any host for the relevant user. **Default**: 1000

Profile Size Limits Window Parameters (continued)

Parameter	Description
Maximum allowed source IP addresses per user	For DB profiles, the maximum number of source IP addresses allowed in a user's profile. When SecureSphere reaches this number, no additional source IP addresses are added to the relevant profile and a warning message is written to the system log. If the profile reaches this limit, consider allowing any IP address for the relevant user. **Default**: 1000
Maximum allowed source OS users per user	For DB profiles, the maximum number of source operating-system user names allowed in a user's profile. When SecureSphere reaches this number, no additional OS user are added to the relevant profile and a warning message are written to the system log. If the profile reaches this limit, consider allowing any user for the relevant user. **Default**: 1000
Maximum allowed hosts per application	For DB profiles, the maximum number of hosts in a profile. When SecureSphere reaches this number, no additional hosts are added to the profile, and they also cannot be learned. **Default**: 4000
Maximum allowed URLs per directory	For Web profiles, the maximum number of URLs profiled in each directory. **Note:** The limit defined by this parameter is not enforced when URLs are added manually, only when they are learned. **Default**: 500
Maximum allowed queries per application	For DB profiles, the maximum number of queries allowed per profile. When SecureSphere reaches this number, no additional queries are added to the profile. **Default**: 3000
Maximum allowed parameters per URL	For Web profiles, the maximum number of different parameter names allowed per URL in the profile. When SecureSphere reaches this number, a certain percentage of the URL's parameters are deleted and a warning message is written to the system log. If these deletions occur repeatedly you should check whether some parameter names are dynamically generated by the application. In this case the profile will never stop growing and you should add a parameter prefix that matches all dynamic parameters. SecureSphere automatically generates parameter prefixes for parameters which start with letters and end with numbers. **Note:** The limit defined by this parameter is not enforced when parameters are added manually, only when they are learned. **Default**: 200

Profile Size Limits Window Parameters (continued)

Parameter	Description
Maximum allowed parameters per application	For Web profiles, the maximum number of different parameter names allowed for each application in the profile. If these deletions occur repeatedly you should check whether some parameter names are dynamically generated by the application. In this case the profile will never stop growing and you should add a parameter prefix that matches all dynamic parameters. Note that SecureSphere automatically generates parameter prefixes for parameters which start with letters and end with numbers. Consult Imperva support before changing this value. **Note:** The limit defined by this parameter is not enforced when parameters are added manually, only when they are learned. **Default**: 3000
Maximum allowed URLs per application	For Web profiles, the maximum number of URLs in each profile. **Note:** The limit defined by this parameter is not enforced when URLs are added manually, only when they are learned. **Default**: 5000
Maximum allowed sub-directories per directory	For Web profiles, the maximum number of sub-directories allowed in a single directory in a server group's profile. When SecureSphere reaches this number, no additional sub-directories are added to the relevant directory and a warning message is written to the system log. Note that by default SecureSphere does not profile static URLs (such as image files) so only directories that include dynamic URL such as ASP and JSP files are counted. If the profile reaches this limit you should first check whether some directory names are dynamically generated by the application. In this case the profile will never stop growing and you should consider adding a URL pattern (prefix or suffix) which matches all dynamic directories. **Default**: 500
Maximum allowed parameters per SOAP action	For Web profiles, the maximum number of different parameter names allowed for each SOAP Action in the profile. When this limit is exceeded, no additional elements will be added to the relevant SOAP action and a warning message is written to the system log. **Default**: 100
Maximum allowed database users per application	For DB profiles, the maximum number of database users allowed per profile. **Default**: 100
Maximum database user groups per application	For DB profiles, the maximum number of database user groups allowed per profile. **Default**: 100

Profile Size Limits Window Parameters (continued)

Parameter	Description
Maximum allowed queries per Query Group	For DB profiles, the maximum number of queries allowed per query group in a server group's profile. When SecureSphere reaches this number, no additional queries are added to the relevant query group and a warning message is written to the system log. By default SecureSphere switches query groups with many queries to Dynamic Protect and stops learning additional queries in these query groups. When the profile reaches this limit, check the recommended mode of this query group. If the recommended mode is Dynamic Protect and the query is in either Static Protect or Learning mode, consider manually switching it into Dynamic Protect. **Default**: 2000
Maximum allowed Query Groups per User	For DB profiles, the maximum number of query groups allowed in a user's profile. When SecureSphere reaches this number, no additional query groups are added to the relevant database user and a warning message is written to the system log. If the profile reaches this limit, check whether some query groups are dynamically generated by the application. In this case the profile will never stop growing and you should add an SQL Text Replacement rule which matches all dynamic SQLs. To define a Text Replacement rule, click **Main** > **Setup** > **Sites**, select a DB service, and click the **Operation** tab. You can define a new rule under **Text Replacement**. **Default**: 500
Maximum allowed SOAP actions per URL	For Web profiles, the maximum number of SOAP actions allowed for each URL in the profile. When this limit is exceeded, no additional SOAP actions are added to the relevant URL's profile and a warning message is written to the system log. **Default**: 100
Maximum allowed cookies per application	For Web profiles, the maximum number of cookies allowed for each profile. When this limit is exceeded, no additional cookies are added. If this limit is repeatedly exceeded, check whether some cookie names are dynamically generated by the application. In this case, the profile will never stop growing and you should consider adding a cookie prefix which matches all dynamic cookies. **Default**: 200
Maximum allowed action URLs per application	For Web profiles, the maximum number of action URLs allowed for each profile. **Default**: 200
Maximum allowed login URLs per application	For Web profiles, the maximum number of login URLs allowed for each profile. **Default**: 200

Switching to Protect Mode Thresholds (SQL)

The Protect mode thresholds determine when a DB profile's components are switched from Learning mode to Protect Mode.



Note: Do not change these values unless you are instructed to do so by Imperva support.

The table below describes the DB-related parameters in this window.

If you change any of these parameters, click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For further information, see the ***SecureSphere User Guide***.

Protect Mode Thresholds (SQL) Window Parameters

parameter	Description
Duration (in hours) without new Query Groups required to close the query group list of a user	If SecureSphere sees no new query groups for a user during this time period, it assumes that it has learned all the query groups for this user and switches the user to Protect mode. You can manually close a users query group list, either completely or only for sensitive tables. For testing purposes (in a lab with low traffic levels) consider changing this limit to 24 to test how the system closes the query group list. The minimum value of this parameter is 24 hours. If it is set to a smaller value, SecureSphere considers it as if it were set to 24 hours. **Default**: 72.0
Duration (in hours) without new table operations required to close a user's operation list	If SecureSphere sees no new table/operations for a user during this time period, SecureSphere assumes that it has learned all the table/ operations for this user and switches the user to Protect mode. New query groups which use existing table/operations continue to be learned. You can manually close a users table/operation list, either completely or only for sensitive tables. For testing purposes (in a lab with low traffic levels) consider changing this limit to 24 to test how the system closes the tables & operations list. The minimum value of this parameter is 24 hours. If it is set to a smaller value, SecureSphere considers it as if it were set to 24 hours. **Default**: 72.0
Duration (in hours) without change required to lock the allowed sources and Database-Schema pairs for a Database User	If SecureSphere sees no new item of a specific attribute for a user in Learning mode, the relevant list is locked. New items that belong to the locked list will generate violations (IP Addresses, Host Names, Source Applications, OS User Names and Databases). **Default**: 120.0
Learn individual queries for regular Query Groups	If not selected, new query groups will immediately be switched to protect mode. This is a global setting which applies to all users, but it can be overriden for specificdatabase profile user group as follows: in the **Main** workspace, click **Profiles** and select a database application in the **Sites** tree. In the **Users** pane, select a user group and, in the **Details** pane, click the **Learning Preferences** tab and under **Learn Individual queries for regular (DML) Query Groups**, select one of the parameters. For more information, see ***SecureSphere User Guide***. **Note:** This feature applies to the profile and does not affect the audit mechanism.

Protect Mode Thresholds (SQL) Window Parameters (continued)

parameter	Description
Number of queries required to switch the "stored procedures" Query Group into Dynamic Protect	When the number of queries in the "stored procedures and other operations" query group exceeds this number, the group is switched to Dynamic Protect mode. This number is by default identical with **Maximum allowed queries per Query Group** defined in the **Profile Size Limits** window; if you reduce **Maximum allowed queries per Query Group**, you should reduce this threshold accordingly. This is a global setting which applies to all users, but it can be overriden for specificdatabase profile user group as follows: in the **Main** workspace, click **Profiles** and select a database application in the **Sites** tree. In the **Users** pane, select a user group and, in the **Details** pane, click the **Learning Preferences** tab and under **Number of queries required to switch the "stored procedures" Query Group to Dynamic Protect**, select one of the parameters. For more information, see ***SecureSphere User Guide***. **Note:** This feature applies to the profile and does not affect the audit mechanism. **Default**: 2000
Number of queries required to switch a regular (DML) Query Group into Dynamic Protect	When the number of queries in a query group exceeds this number, the query group is switched to Dynamic Protect. The assumption is that this query group consists of dynamically generated queries. This parameter applies to all query groups except the "stored procedures and other operations" query group. **Default**: 200
Duration (in hours) without new Query Groups required to close the query group list of a user	The query group learning transition period is the number of hours during which there are no new query groups for a user in learning. After this time, the user's query group list is closed and the user enters protected mode. Once in protected mode, any query group not in the users list will generate a violation. The assumption is that after the learning transition period, the SecureSphere has learned all query groups for this user and can start protecting it. The minimum value of this parameter is 24 hours. If it is set to a smaller value, SecureSphere considers it as if it were set to 24 hours. **Default**: 120 **Note:** You can manually close a users query group list, either completely or only for sensitive tables. For testing purposes (in a lab with low traffic levels) consider changing this limit to 24 to effectively test how the system closes the query group list.
Duration (in hours) without new Users required to close the users list	A Learning mode server group's user list is closed if no new users have been added to the group in this timeframe. The assumption is that SecureSphere has learned all users for this server group and can start protecting it. The minimum value of this parameter is 24 hours. If it is set to a smaller value, SecureSphere considers it as if it were set to 24 hours. **Default**: 168 **Note:** Any new query groups which use existing table/operation combinations can still be learned. You can manually close a users table/operation list, either completely or only for sensitive tables. For testing purposes (in a lab with low traffic levels) consider changing this limit to 24 to effectively test how the system closes the tables and operations list.

Switching to Protect Mode Thresholds (Web)

These thresholds determine when a Web profile's components are switched from Learning mode to Protect Mode.



Note: Do not change these values unless you are instructed to do so by Imperva support..

The table below describes the Web-related parameters in this window.

If you change any of these parameters, click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For further information, see the ***SecureSphere User Guide***.

Protect Mode Thresholds (Web) Window Parameters

Parameter	Description
Traceability Percentage required to switch a cookie into partial Protect mode	These four parameters taken together determine when a cookie is switched from Learning mode. If the parameters **Duration (in hours) required to switch all Cookies to protect or ignored mode** and **Minimum occurrences required to switch a cookie into Protect mode** are both exceeded, then: • If the cookie was not changed during at least the number of sessions defined by **Traceability Percentage required to switch a cookie into partial Protect mode**, the cookie is switched to Protect mode without protection against injection. • If SecureSphere saw the SET cookie command for at least the number of sessions defined by **Traceability Percentage required to switch a cookie into full Protect mode**, and the cookie was not changed during at least the number of sessions defined by **Traceability Percentage required to switch a cookie into full Protect mode**, the cookie is switched to Protect mode with protection against injection. Note that **Traceability Percentage required to switch a cookie into partial Protect mode** and **Traceability Percentage required to switch a cookie into full Protect mode** are percentages, not absolute numbers, and relate to a percentage of the total sessions seen by SecureSphere. The minimum value of **Duration (in hours) required to switch all Cookies to protect or ignored mode** is 24 hours. If it is set to a smaller value, SecureSphere considers it as if it were set to 24 hours. **Defaults**: **Traceability Percentage required to switch a cookie into partial Protect mode**: 95.0 **Traceability Percentage required to switch a cookie into full Protect mode**: 95.0 **Duration (in hours) required to switch all Cookies to protect or ignored mode**: 240.0 **Minimum occurrences required to switch a cookie into Protect mode**: 10
Traceability Percentage required to switch a cookie into full Protect mode	
Duration (in hours) required to switch all Cookies to protect or ignored mode	
Minimum occurrences required to switch a cookie into Protect mode	

Protect Mode Thresholds (Web) Window Parameters (continued)

Parameter	Description
Duration (in hours) required to switch all URLs to Protect mode	A URL is automatically switched to Protect mode based on the following factors: • the number of occurrences in the traffic • whether the URL has parameters • the time passed since it was first seen by SecureSphere The more frequently the URL occurs in traffic, the sooner it is switched to Protect mode. This parameter specifies the number of hours since the first time this URL was seen after which the URL is automatically switched to Protect mode, without regard to the number of its occurrences in the traffic or whether it has parameters. **Default**: 240.0
Success rate required to set a specific parameter as read-only	If a parameter has been seen **Number of occurrences required to determine if a parameter is read-only** times, it is set to read-only, if in **Success rate required to set a specific parameter as read-only** percent of the time it was successfully identified as read-only. If you are testing the system in a lab with a low amount of traffic, consider changing this parameter to 50, in order to be able to test the system and the way it sets parameters as read-only. The lower this number, the greater the chances of false positives and false negatives. **Default**: 99.9
Number of occurrences required to determine if a parameter is read-only	See the previous parameter. If you are testing the system in a lab with a low amount of traffic, consider changing this parameter to 6 in order to be able to test the system and the way it sets parameters as read-only. The lower this number, the greater the chances of false positives and false negatives. **Default**: 10

Gateway Settings

This section describes the windows related to gateways, and includes:

Audit Settings on page 296
Response Page Display in Alerts Settings on page 296
Web to Database User Tracking Settings on page 296

Audit Settings

These parameters relate to auditing of responses and paths.

Audit Settings Window Parameters

Parameter	Description
Enable support for queries or full-paths larger than 4k	When enabled, the SecureSphere gateway preserves the entire path or query regardless of size. If not enabled, only the first 4K of queries or paths are preserved.
Collect audit data from unapplied policies	When enabled, SecureSphere collects audit data from all Gateways, including Gateways on which the audit policy is not applied. This option is useful if the audit policy has been unapplied from some Gateways, in which case these Gateways may be holding relevant audit data even though the policy is no longer applied on them. When not enabled, SecureSphere collects audit data only from Gateways on which the audit poicy is currently applied. This parameter affects the policies which are displayed in the following windows: • **Policy** in the **Scope** pane of **Main** > **Audit** > **DB/File/SharePoint Audit Data**. • **Policies** in the **Data Scope** tab of **Main** > **Reports** > **Manage Reports**.

Response Page Display in Alerts Settings

These parameters relate to the display of response pages.

If you change any of these parameters, click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the ***SecureSphere User Guide***.

Response Page Display in Alerts Settings Window Parameters

Parameter	Description
Maximal disk space on gateway for responses	Maximum disk space on gateway that will be allocated for responses (in MB). When this disk space fills up, new response pages will overwrite old ones. **Default**: 5000 MB
Maximal response page size	The maximum response page size (in KB.) **Default**: 1000 KB

Web to Database User Tracking Settings

These parameters define the web to database user tracking functionality. You should consult with Imperva support before changing any of these parameters.

If you change any of these parameters, click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the ***SecureSphere User Guide***.

Web to Database User Tracking Settings Window Parameters

Parameter	Description
Learning Mode	This parameter defines a balance between the speed of learning and its accuracy. Choose one of the following options: • **Quick**: Learn quickly but with a loss of accuracy. This is the default. • **Refined**: Monitor activity over a greater length of time in order to improve accuracy. The correlation requires more repeated confirmations before it is learned. The learning process is slower, but it is more accurate.
Maximum Pending Request Time (seconds)	Web to Database User Tracking matches the start of an HTTP request to the data returned (ultimately from SQL statements) in response to the request. This parameter defines the maximum time SecureSphere will wait before concluding that there was no response to the request. The default value (10 seconds) is very “patient”, which allows for delayed topology options such as using a SecureSphere remote agent in Global Mode to send correlation packets to the SecureSphere gateway.
Pending HTTP Request End At	This parameter defines the event at which the request ends. Choose one of the following options: • **Response Headers** • **Response Data Start** • **Response Complete**
Pending HTTP Request Start At	This parameter defines the event at which the response begins. Choose one of the following options: • **Request Complete** • **Request Headers**

Security and Authentication

This section describes the windows related to security and authentication, and includes:

Authentication and Authorization Configuration on page 298
FIPS Settings on page 298
Password Settings on page 299
SSL Certificate Expiration Monitoring on page 300

Authentication and Authorization Configuration

The **Authentication and Authorization** configuration includes the following two parts:

- In the **Authentication** section, add username and password to identify the user.
- In the **Authorization** section, define the process of granting roles and permissions for SecureSphere/ external system users.

To configure user authentication:

1. In the **Admin** workspace, select **System Definitions** > **Authentication & Authorization Configuration**. The **Authentication & Authorization Configuration** pane appears.
2. For **User Authentication** , select one of the following options:
   - **SecureSphere**: Allows authenticating using the internal SecureSphere database only.
   - **External**: Allows authenticating using external authentication systems. If you select this option, you must select the external system from the **External Authentication System** dropdown list. The external systems that you can choose from are defined in the **External Systems** pane, see External Systems on page 307.
   - **User Specific**: Allows authenticating using SecureSphere database or external authentication systems. If you select this option, you must select the external system from the **External Authentication System** dropdown list. The external systems that you can choose from are defined in the **External Systems** pane, External Systems on page 307.
3. To enable managing SecureSphere users in LDAP, select **External Authorization**. The LDAP group permissions are reflected in the SecureSphere external role permissions. For **External Authorization System**, select an external system from the dropdown list.

   For information about external systems, see External Systems on page 307.



Notes:

- When de-selecting the External Authorization option, all the external users are moved to the regular users section in the **Users & Permissions** window. They maintain their external system authentication, but lose their external role assignment.
- When selecting the **External Authorization** option, all Users with external system authentication become externally authorized: they are moved to the External Users section in the Users & Permissions window, and their permissions are based on their External Roles.

4. Click **Save**.

FIPS Settings

This parameter relates to FIPS (Federal Information Processing Standard) 140-2.

For more information about SecureSphere FIPS 140-2 compliance, see Appendix F, FIPS 140 Compliance.

If you change this parameter, click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the ***SecureSphere User Guide***.

FIPS Settings Window Parameters

Parameter	Description
FIPS Mode	If enabled, the Management Server and the Gateways will communicate in a manner compliant with the FIPS 140-2 standard. For more information about FIPS 140 standard, see Appendix F, FIPS 140 Compliance. **Default**: not selected

Password Settings

These parameters define requirements for passwords of SecureSphere users and administrators.

These settings apply only to internal SecureSphere users and administrators, that is, the ones defined in the SecureSphere GUI. For more information, see Understanding Permissions on page 228.

If you change any of these parameters, click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the ***SecureSphere User Guide***.

Password Settings Window Parameters

Parameter	Description
Password validity period (in days): Passwords expire at the end of this period	The number of days after which a password expires. At the end of this period, the user or administrator is required to change the password. **Default**: 100 days
Password length: Minimum required number of characters in a password	The minimum length of a password (in characters). **Note:** The longer the password, the more difficult it is to guess. **Default**: 7 characters
A password must be significantly different from last password used	Specifies whether a new password must be significantly different from the password it replaces. **Note:** If a new password is significantly different from the password it replaces, knowledge of the previous password does not confer an advantage on attackers. **Default**: not selected
A password must include capital letters	Specifies whether a password must include at least one upper-case character. **Default**: not selected
A password must include numbers	Specifies whether a password must include at least one numeric character. **Default**: selected
A password must include lower case letters	Specifies whether a password must include at least one lower-case character. **Default**: selected
A password must include non alpha-numeric characters	A password must include one of the following characters: ! @ # $ % ^ & * ( ) < > ? . _ + = - [ ] { } \ | : ; , / ` ~ **Default**: not selected



Note: The longer a password and the greater the variety of its required characters, the more difficult it is to guess.

For more information about user permissions, see Understanding Permissions on page 228.

SSL Certificate Expiration Monitoring

Every night at 23:00 SecureSphere scans the SSL keys and identifies those keys about to expire and those which have already expired (including an optional grace period). The parameters below define the deletion process.

In the **SSL Settings** pane, configure the options.

SSL Settings Pane Parameters

Parameter	Description
Number of days before SSL key expiration to issue system event warning	The number of days before an SSL key's expiration date on which to issue a low-severity system event warning. If empty, no warnings are issued. **Default**: None
Expired SSL key deletion grace period	The number of days after an SSL key's expiration date on which to delete the key. If **Expired SSL key deletion grace period** is not empty: • Expired keys are deleted after the grace period has passed. • A system event is issued for keys that expire on the date of the scan. If **Expired SSL key deletion grace period** is empty, no keys are deleted and no systems events are issued. **Default**: None

If both fields are empty, the scan is not run.

Management Server Settings

This section describes the windows related to management servers, and includes:

Action Interfaces on page 301
Agents on page 303
Alert Aggregation Configuration on page 304
Application Groups Settings on page 305
Assessments on page 305
CSV Upload Default Settings on page 305
Data Owner Settings on page 306
External HTTP Settings on page 306
External Systems on page 307
Keywords Settings on page 317
Log Collectors on page 319

Action Interfaces

Parameters of the following Action Interfaces are defined in the **Action Interfaces** window:

1. Archive to an FTP Location
2. Archive to an SCP Location
3. Assign as Task
4. Block a User
5. Block an HTTP Session
6. Block an IP (Address)
7. Create a Review Task
8. Log DAM audit events to System Log (Gateway syslog) using the CEF standard
9. Log FAM audit events to System Log (Gateway syslog) using the CEF standard
10. Log SharePoint audit events to System Log (Gateway syslog) using the CEF standard
11. Log audit events to System Log (Gateway syslog)
12. Log custom security event to System Log (syslog) using the CEF standard
13. Log network security event to System Log (syslog) using the CEF standard
14. Log security event to RSA enVision
15. Log security event to System Log (syslog) using the CEF standard
16. Log system event to RSA enVision
17. Log system event to System Log (syslog) using the CEF standard
18. Log to System Log (syslog)
19. Monitor a User
20. Monitor an HTTP Session
21. Monitor an IP (Address)
22. Remedy Create Incident
23. Run a Shell Command
24. SNMP Trap
25. Send an Email
26. Terminate Session

The parameters in all these windows are explained in “Working with Action Sets and Followed Actions” in the ***SecureSphere User Guide***.

The windows here (**Admin** > **System Definitions** > **Action Interfaces**) enable an administrator to:

- define Action Interfaces
- pre-define a value for an Action Interfaces parameter used in Action Sets by deselecting **User-Configured** for that parameter, so that when a user includes the Action Interface in an Action Set (**Main** > **Policies** > **Action Sets**), the values of these parameters are pre-defined in the Action Interface and the user cannot change them.

For example, if the Action Interface **Send an Email** is defined, then when the user defines an Action Set which includes it, the **SMTP Server Address** is pre-defined and the user cannot change its value.

This is illustrated in Figure 60 and Figure 61 below.

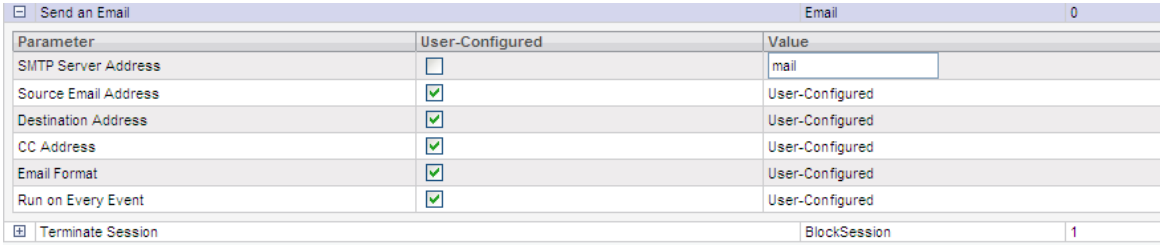


Figure 60 Send Email Action Interface

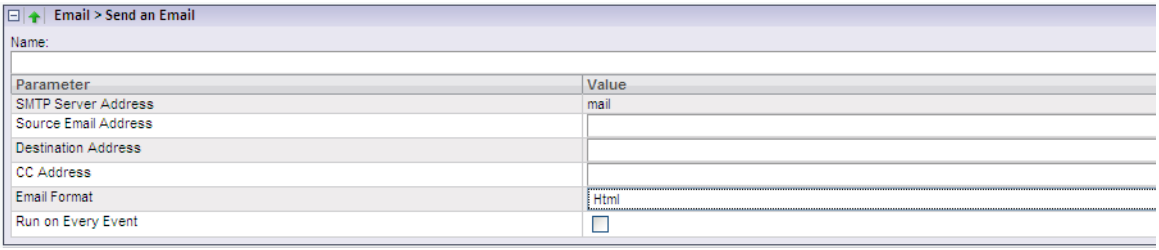


Figure 61 Send an Email used in an Action Set

In the Interfaces pane:

- The **Type** column specifies in which types of objects the Action Interface can be used.
- The **Usage Counter** column specifies the number of Action Sets in which the Action Interface is used.

Note: For most Types, there are pre-defined Action Interfaces. For the Types HTTP Archive, HTTPS Archive and NFS Archive, no Action Interfaces are pre-defined, but administrators can create new Action Interfaces of these Types.

Creating and Configuring Action Interfaces

You can create a new Action Interface, or edit and delete an existing one.

To create a new Action Interface:

1. In the **Admin** workspace, click **System Definitions**.
2. In the **System Definitions** pane, select **Action Interfaces**.
3. In the **Interfaces** pane, click .
4. Enter the Action Interface's **Name**.

   Name should be meaningful, because the Action Interface will be used in Action Sets.
5. Select the Action Interface's **Type** from the drop-down list.

   An Action Interface's **Type** determines the Action Set event types in which it can be used.

   For more information, see "Working with Action Sets and Followed Actions" in the **SecureSphere User Guide**.
6. Click **Create**.

7. When the new Action Interface is displayed in the list, expand it by clicking on the plus-sign to the left of its name.
8. Edit the Action Interface's parameters.

   To pre-define a value for one of the Action Interface's parameters, deselect **User-Defined** for that parameter and enter a value. If you select **User-Defined**, the user will have to specify a value for the parameter when defining an Action Set that uses this Action Interface.

   See Working with Action Sets and Followed Actions in the **SecureSphere User Guide**.
9. Click **Save**.

Settings are saved. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the **SecureSphere User Guide**.

To edit an existing Action Interface:

1. In the **Admin** workspace, click **System Definitions**.
2. In the **System Definitions** pane, select **Action Interfaces**.
3. In the **Interfaces** pane, select an Action Interface from the list.
4. Expand the Action Interface by clicking on the plus-sign to the left of its name.
5. Edit the Action Interface's parameters.

   To pre-define a value for one of the Action Interface's parameters, deselect **User-Defined** for that parameter and enter a value. If you select **User-Defined**, the user will have to specify a value for the parameter when defining an Action Set that uses this Action Interface.

   For more information, see Working with Action Sets and Followed Actions in the **SecureSphere User Guide**.
6. Click **Save**.

Settings are saved. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the **SecureSphere User Guide**.

To delete an existing Action Interface:

1. In the **Admin** workspace, click **System Definitions**.
2. In the **System Definitions** pane, select **Action Interfaces**.
3. In the **Interfaces** pane, select an Action Interface from the list.
4. Click  .
5. Click **Save**.

Settings are saved. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the ***SecureSphere User Guide*.**

Agents

This parameter relates to Remote Agents.

If you change this parameter, click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the ***SecureSphere User Guide.***

Agents Window Parameters

Parameter	Description
Apply default services to new agents according to protected IPs	If enabled, a newly-defined Remote Agent will monitor the database service previously defined as protected by the SecureSphere Gateway, provided that exactly one database service is defined for the Gateway (group). **Default**: enabled
Deletion interval for automatically discovered installed certificates	Automatically discovered installed certificates will be deleted after the specified number of days after the first time the Remote Agent does not discover them. **Default**: 90 days

Alert Aggregation Configuration

These parameters define how alerts are aggregated.

If you change any of these parameters, click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the **SecureSphere User Guide**.

Alert Aggregation Configuration Window Parameters

Parameter	Description
Alert aggregation mechanism is active	Enable this parameter in order to activate the alert aggregation mechanism. **Warning**: Disabling this parameter will cause SecureSphere to produce large number of alerts of the same type. **Default**: enabled
Maximal no. of regular alerts that can be aggregated into a single alert	When an aggregated regular (non-monitoring) alert reaches this limit, no new alerts will be aggregated to it. **Default**: -1 (meaning there is no limit)
Maximal no. of monitoring alerts that can be aggregated into a single alert	When an aggregated monitoring alert reaches this limit, no new alerts will be aggregated to it. **Default**: -1 (meaning there is no limit)
Maximal no. of detailed alerts kept per aggregated alert	When alerts are aggregated, SecureSphere stores, in addition to the aggregated alert information, a certain number of unaggregated alerts, which you can see in the alert viewer when browsing the aggregated alert. This parameter limits the number of raw alerts kept per aggregated alerts. Increase this value with caution, as large values may result in a very quick growth of the database, and will cause the system to discard old alerts more frequently in order to make room for new alerts. **Default**: 30

Application Groups Settings

This parameter relates to whether the Sites hierarchy or the Application Group hierarchy is used to apply policies.

If you change this parameter, click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the **SecureSphere User Guide**.

Applications Groups Settings Window Parameters

Parameter	Description
Apply application-level policy objects using application group hierarchy	Use the Application Group hierarchy rather than the Sites hierarchy. **Default**: not selected **Note:** A site can be organized either based on a server group hierarchy (**Main** > **Setup** > **Sites**) or on an application hierarchy (**Main** > **Setup** > **Applications**), but not both. Once the decision has been made, the organization cannot be changed, that is, the site cannot be migrated from one hierarchy to the other.

Assessments

This parameter relates to whether legacy assessment tests are enabled. For more information, see Pre-Defined Assessment Policies on page 190.

If you change this parameter, click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the ***SecureSphere User Guide***.

Assessments Window Parameters

Parameter	Description
Assessment Record Results Limit	Assessment record results limit. **Default**: 1000
Legacy Assessment Tests	Enable **Value** to enable legacy assessment tests. **Default**: not selected

CSV Upload Default Settings

This parameter relates to the CSV Upload Settings when uploading IP Groups and Protected IP Addresses.

If you change this parameter, click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the ***SecureSphere User Guide***.

Assessments Window Parameters

Parameter	Description
Case Sensitive	Specifies whether the data in the CSV file are case sensitive, so if exisitng data match the data in the CSV file, they are not considered duplicates.

Assessments Window Parameters (continued)

Parameter	Description
Encoding	Select either **ASCII** or **UTF8**.
Format	Select **UNIX** or **Windows**.
Use First Line As Header	Specifies whether the first line of the CSV file contains data to be imported or column headings.
Override Existing Entries	If the data in the CSV file matches existing data, then the data in the CSV file will overwrite the exiting data.

Data Owner Settings

These parameters relate to the Data Usage feature. If this feature is enabled, FAM collects usage statistics and suggests data owners for folders and files based on the frequency with which specific users access the folders and files. These suggestions can be accepted or rejected by the SecureSphere administrator. The collected usage statistics are used for URM audit enrichment.

Data Usage Window Parameters

Parameter	Description
Disabled	If selected, SecureSphere will not collect audit statistics and will not suggest data owners for files and folders. This setting also affects the URM audit enrichment functionality.
Verify Owner	If selected, then when a SecureSphere administrator assigns a data owner, SecureSphere will check whether the user exists in LDAP.
Save Data Usage for Folders Only	If selected, FAM will suggest owners only for folder but not files, in order to reduce the amount of data processed.
Tree Depth	If specified, FAM will suggest owners for folders (and files, if **Save Data Usage for Folders Only** is not checked) only to the specified depth.

External HTTP Settings

To perform various updates SecureSphere needs to establish an Internet connection. The External HTTP Settings capability is used to establish the Internet connection using a proxy. The following updates can be performed:

- ADC content updates
- Web scanners updates
- ThreatRadar updates

To configure an Internet connection using HTTP proxy:

1. In the **Admin** workspace, click **System Definitions**.
2. From the **System Definitions** pane, select **External HTTP Settings**. The **External HTTP Settings** pane appears on the right.
3. Enter the parameters as described below.

Parameter	Description
Ignore HTTP Certificate	Specify whether to ignore the HTTP certificate.
HTTP Proxy Configuration	Select to enable the following parameters.
IP	Enter the proxy's IP address.
Port	Enter the proxy's port, for example, 80 for HTTP or 443 for HTTPS.
Authentication Policy	Select an authentication protocol from the dropdown list.
User / Password / Verify Password	Enter the username and the password defined for SecureSphere user account on the proxy server.
Domain	When the NTLM is selected as the Authentication policy, you must specify the domain.

4. Click **Save**.

External Systems

These parameters specify how to connect to the lookup dataset and also define external systems that can be used in the SecureSphere login process to use the external system, it must be enabled in the External Sytems pane.

For information about lookup datasets, see the Advanced Configuration chapter in **SecureSphere User Guide**. For information about the authentication configuration see Authentication and Authorization Configuration on page 298.

If you change these parameters, click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the ***SecureSphere User Guide***.

Defining External Systems

You can create a new External System, or edit and delete an existing one.

To create a new External System:

1. In the **Admin** workspace, click **System Definitions**.
2. In the **System Definitions** pane, select **External Systems**.
3. In the **External System** pane, click  . The **External Systems** window appears.
4. In the **Name** text box, enter the name for the external system.
5. From the **Type** drop-down list, select one of the following options:

Active Direction Collection	Describes how to configure Domain Forests, known as Active Directory Collections in SecureSphere. For more information see External Systems - Active Directory Collection (Forest) on page 309.
Kerberos Authentication	Describes how to configure SecureSphere to connect to the Kerberos domain account and authenticate users so they don't need to login with a user and password. For more information see External Systems - Kerberos Authentication on page 310.

LDAP	For more information, see External Systems - LDAP on page 313.
LDAP Authentication & Authorization	For more information, see External System - LDAP Authentication and Authorization on page 313.
RADIUS Authentication	For more information, see External System - RADIUS Authentication on page 315.
SQL	For more information, see External System - SQL on page 316.
SSL Proxy	For more information, see External System - SSH Proxy on page 316.

6. If you change any of these parameters, click **Save**.

   If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the **SecureSphere User Guide**.

To edit an existing External System:

1. In the **Admin** workspace, click **System Definitions**.
2. In the **System Definitions** pane, select **External Systems**.
3. In the **External System** pane, select an External System from the list.
4. Expand the External System by clicking on the plus-sign to the left of its name.
5. Edit the External System's parameters.

   See External Systems - LDAP on page 313 for an explanation of External System parameters.
6. If you change any of these parameters, click **Save**.

   If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the **SecureSphere User Guide.**

To delete an existing External System:

1. In the **Admin** workspace, click **System Definitions**.
2. In the **System Definitions** pane, select **External Systems**.
3. In the **External System** pane, select an External System from the list.
4. Click .
5. Click **Save**.

   If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the **SecureSphere User Guide**.

External Systems - Active Directory Collection (Forest)

SecureSphere supports the use of Domain Forests. In SecureSphere, this feature is known as Active Directory Collections. By configuring an Active Directory Collection you enable the system to integrate user information across various Active Directory domains. Members of the collection can be from different forests as long as they have two way trust.

For information on creating and managing an Active Directory Collection external system, see Defining External Systems on page 307.

Active Directory Collection Configuration Parameters

Parameter	Description
Available LDAP System	Lists the various LDAP systems that have been configured in SecureSphere.
Collection Members	Lists those LDAP systems you have selected to participate in the LDAP Collection (members of the forest). **Note:** Using the Test Connection button, you can test connections to all enabled members after saving.

External Systems - Kerberos Authentication

SecureSphere enables you to configure connectivity with your Kerberos Domain account to enable Windows users to be automatically logged into SecureSphere through Kerberos and subsequently eliminate the need for them to type their username and passwords.

This procedure describes how to configure the required components in order to support this form of authentication. Kerberos involves the following primary steps:

Table 7 Configuring Automatic Kerberos Authentication

	Action	Description	For more information, see...
1	**Setup the Domain Controller**	Configure the Service Principal on the domain controller and generate a keytab file for import into SecureSphere.	See your Windows server documentation for assistance.
2	**Add Hostnames and IP addresses to Domain Controller**	Configure your Domain Controller with hostnames and IP addresses	See your Domain Controller documentation for assistance
3	**Configure Browsers**	Configure the browser you want to use to access SecureSphere.	Configuring the Browser for Kerberos Authentication on page 311
4	**Configure SecureSphere**	Configure SecureSphere Admin definitions required to support authentication.	Configuring SecureSphere for Automatic Kerberos Authentication on page 312

Supported Components

Kerberos Authentication is Supported with the following components

Components	Supported Versions
Servers	**Win2003, Win2008**
Clients	**WinXP, Win7, Vista, Win2000**
Browsers	**Internet Explorer versions 6,7,8 and 9** **Firefox versions 3, 3.6 and 4** **Chrome (latest)** **Safari (latest)**

Configuring the Browser for Kerberos Authentication

The first step in configuring kerberos authentication and enabling users to access SecureSphere and be automatically authenticated using Kerberos (and not need to type a username and password), involves making some minor changes in the browser.



Notes:

- When logging in, users must navigate to the host name of the SecureSphere server. Navigating to the IP address will not enable them to automatically log in and they will be asked for credentials.
- Clients must be in the same domain of the Domain Controller, or in a domain with a trust or sub-domain.
- When users are in a domain with trust, they need to navigate using the SecureSphere server hostname + full domain. For example, https://MX_hostname.domain.com:8083/

Currently, Kerberos authentication requires configuring the browser:

- **Windows IE**: see Configuring Windows Internet Explorer (IE) for Kerberos Authentication on page 311
- **Firefox**: see Configuring Firefox for Kerberos Authentication on page 311

Configuring Windows Internet Explorer (IE) for Kerberos Authentication

This procedure describes how to configure Windows IE to support Kerberos authentication to SecureSphere. For instructions on how to configure Firefox, see Configuring Firefox for Kerberos Authentication on page 311.

To configure Windows IE:

1. In **Windows IE**, from the **Tools** menu, click **Internet Options**. The **Internet Options** window opens.
2. Click the **Security** tab.
3. Select the **Local Intranet** zone, then click the **Sites** button. The **Local Intranet** window opens.
4. Click **Advanced**, advanced settings are displayed.
5. Type the fully qualified URL for the website that is to be authenticated using Kerberos.

   For example: http://mywebsite.mycompany.com
6. Click **OK**.
7. Configure SecureSphere settings as described in Configuring SecureSphere for Automatic Kerberos Authentication on page 312.

Configuring Firefox for Kerberos Authentication

This procedure describes how to configure Firefox to support Kerberos authentication to SecureSphere. For instructions on how to configure Windows IE, see Configuring Windows Internet Explorer (IE) for Kerberos Authentication on page 311.

To configure Firefox:

1. Open **Firefox**.
2. In the **Address** bar, type **About:Config**. You are displayed a warning message. Click **I'll be careful, I promise**. Configuration settings are displayed.
3. Find the Preference Name **network.negotiate-auth.trusted-uris** and double-click it. The **Enter String Value** window opens.
4. Type the Domain for the website that is to be authenticated using Kerberos.

   For example: il.imperva.com
5. Click **OK**. Settings have been changed.
6. Configure SecureSphere settings as described in Configuring SecureSphere for Automatic Kerberos Authentication on page 312.

Configuring SecureSphere for Automatic Kerberos Authentication

In order to support Kerberos Authentication of SecureSphere users you need to configure settings in the Admin workspace of SecureSphere.



Note: Time needs to be synched between clients, the SecureSphere Server, and the Domain Controller using the same timeserver.

To configure SecureSphere Kerberos Admin settings:

1. In the **Admin** workspace, click **System Definitions > External Systems**. External Systems are displayed.
2. In the **External System** pane, Click **New**. The New External System window opens.
3. Type a **Name** for the External System, select **Kerberos Authentication** from the dropdown menu, then click **Create**. A new **External System** is added to the **Details** pane.
4. Expand the **External System** by clicking on the plus-sign to the left of its name.
5. Click **Upload Kerberos Details**. Then do the following:
   - In the **Service Principal** field, type the **Service Principal Key** you configured in the Domain Controller. Syntax of Service Principal username@mycompany.com.
   - Under **File**, click **Browse**, navigate to the location of your **Keytab file**.
   - Click **Upload**.

   Note: For instructions on obtaining a Service Principal name or generating a Keytab file, see your Domain Controller documentation, or refer to the Imperva Support Knowledge Base.
6. Under **Username Type,** select a **Username Type**. This option represents the how user names are formatted in SecureSphere. Select one of the following:
   - **Username with domain**: Select this option when SecureSphere usernames are required to have domain names attached. For example, if your user name is JamesT and your company name is Company. Users must type in JamesT@Company.com
   - **Username without domain**: Select this option when using internally when no domain is required as part of the username. Using the above example, your user would type in JamesT.

   Note: If there's the possibility that you have two users from different domains with the same username, be sure your system is configured to use Usernames with domains.
7. Click **Save**.
8. Enable the external system be selecting the **Enabled** checkbox.
9. Click **Save**.
10. In the **System Definitions** tree in the left-hand side of the window, click **Authentication Configuration**.
11. In the **Details** pane, click one of the following:
    - **External**: Authenticating with an external system such as Radius, LDAP and Kerberos
    - **User Specific**: Takes the settings as configured in the Authenticator field of the User Information Tab under **Users and Permissions**.
12. Select the **External System** you configured in step 2. above.
13. Click **Save**.

    You can now create users in the Users and Permissions section of the Admin workspace. These users need to match the ones you created on your Domain Controller.

External Systems - LDAP

You can define the LDAP external system.

The connection can be established once this external system is enabled.

LDAP configuration Parameters

Parameter	Description
Name	The external system's name.
Primary Server	The IPv4 or IPv6 address or the host name of the primary external system.
Secondary Server	The IPv4 or IPv6 address or the host name of the secondary external system.
Use SSL	Specifies whether to connect to the external system using SSL.
Port	The port number on the external system.
Account Name DN	The account name or DN (Distinguished Name) under which to connect to the external system.
Password	The password to use when connecting to the external system.
Verify Password	Re-enter the password.
Base DN	The Base Distinguished Name is the domain account name in the LDAP server's navigation tree.
Follow Referrals	Select this option to tell/direct the LDAP system to follow referrals.

Click **Test Connection** to verify that the connection to the external system is functioning properly.

External System - LDAP Authentication and Authorization

You can set the parameters related to LDAP authentication & authorization of SecureSphere users.

The connection can be established once this external system is enabled.

If you change any of these parameters, click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the ***SecureSphere User Guide***.



Note:

- The admin user cannot be authenticated using LDAP, but is always authenticated by SecureSphere.
- When configuring the external system using a hostname, and not an IP address: In order to use LDAP to authenticate SecureSphere users, a DNS client must be enabled on the management server using the `impcfg` command. For more information, see Name Resolution (DNS client) on page 90.

LDAP Authentication Window Parameters

Parameter	Description
Connection Settings	
Name	The external system's name.
Primary LDAP Server Host	The IP address or the host name of the primary LDAP server.
Port	The port number of the LDAP service on the primary LDAP server.

LDAP Authentication Window Parameters (continued)

Parameter	Description
Secondary LDAP Server Host	The IP address or the host name of the secondary LDAP server.
Port	The port number of the LDAP service on the secondary LDAP server.
Use SSL	Select to specify that communication with LDAP servers is encrypted. If this option is selected, ensure that the port number is changed accordingly.
Access Mode These parameters specify whether access to the LDAP server is anonymous or conducted under a specific user. Select one of the following:	
Anonymous	Use the “guest” account on the LDAP server, if it is configured.
User Account	If **User Account** is selected, then the following parameters must be defined: • **Account DN**: The Distinguished Name of the domain account under which the LDAP server is to be accessed. • **Password**: The domain account’s password. • **Verify Password**: Re-enter the password.
Search Settings The following parameters define how to locate a user in LDAP.	
Identifier Field	Enter the unique identifier that SecureSphere uses to identify the external LDAP users. If **Identifier Field** is empty, the user name in SecureSphere is the same as on the LDAP server. **Note:** Case-Sensitivity: Depending on the LDAP server, the login process (authentication by sam-name/email, etc.) may or may not be case-sensitive. However regarding **Identifier Field** vs. name, the comparison in SecureSphere is case-sensitive (this is a cross-system behavior). For example if the user CN in LDAP is "John Smith", you must set the SecureSphere user name to "John Smith" not "john smith". Default: CN.
Base Path for Users	The domain path in the authentication server's navigation tree where the LDAP users are stored. **Note:** You can set this parameter only when the External Authentication parameter is enabled, see step 3. on page 298.
Search Filter	The search criteria for the unique identifier. **Note:** If you change the search filter in your authentication server's account (for example, from username to email) users will then have to use a different login name.
Users Search Scope	Select one of the following: • **One Level**: Limits the search to the base path only. • **Subtree:** Allow searching subtree branches.
Authorization Settings	
Enable	Enables reflecting LDAP permission group structure in SecureSphere, where LDAP groups are mapped to SecureSphere external roles.
Base Path for LDAP Groups	The domain path in the authentication server's navigation tree where the LDAP groups are stored. **Note:** You can set this parameter only when the External Authentication parameter is enabled, see step 3. on page 298.

LDAP Authentication Window Parameters (continued)

Parameter	Description
Groups Search Scope	Select one of the following: • **One Level**: Limits the search to the base path only. • **Subtree:** Allow searching subtree branches.

Click **Test Connection** to verify that the connection to the LDAP servers is functioning properly.



Note: To point SecureSphere to the Active Directory Global Catalog, set **Base Path** to the domain root (for example, DC=corpmain,DC=com) and **Port** to 3268.

To view or modify the LDAP authentication configuration for individual users:

1. In the Admin workspace, click **Users & Permissions**.
2. In the **List** pane, select a user.
3. Click the **Details** tab.
4. To specify that this user is to be authenticated externally, select **External** under **Authenticator**.
5. If you want to check if this user exists on the authentication server, click **User Lookup**.
6. The **LDAP User Lookup** dialog box appears.
7. Type the username of the LDAP user to search for and click **Search**. The **Test User** progress bar appears.

Third-Party Authentication Task Flow:

1. Obtain the enterprise account details (server's IP addresses, domain account name to be used for authentication, its password, etc.) from your Domain Administrator.
2. Configure the system for third-party authentication (in the GUI: **Admin** > **System Definitions** - **Authentication & Authorization Configuration**).
3. Configure the users who are to be authenticated via third-party authentication (in the GUI: **Admin** > **Users & Permissions** - click the create new icon or select the user and click the **Details** tab).

External System - RADIUS Authentication

You can define the RADIUS external system to connect to the RADIUS server.

The connection can be established once this external system is enabled.

RADIUS Authentication Parameters

Parameter	Description
Name	The external system's name.
Primary Server	The IP address or the host name of the primary external system.
Secondary Server	The IP address or the host name of the secondary external system.
Primary/Secondary Server Port	The port number on the external system used by primary/secondary server. Default: 1812.
Shared Secret	The shared password to use when connecting to the RADIUS server.
Verify Shared Secret	Re-enter the password.

RADIUS Authentication Parameters (continued)

Parameter	Description
Authentication Protocol	The authentication method that is used to establish the connection with the RADIUS server.
Additional Attributes	Provide the RADIUS attributes which should be specified to communicate with the RADIUS server. For each attribute, provide the following: • **Id**: The attribute Id refers to the numerical value of the "RADIUS attribute Type" as defined by RADIUS RFC 286, section 5 (http://tools.ietf.org/html/rfc2865). For example, the Id of Attribute "NAS-IP-Address" is 4, the id of attribute "Service-Type" is 6 and so on. • **Value**: When providing values for the attributes which have a fixed set of predefined values (for example: "Service Type"), please provide the numeric ID of the value (as defined in the RFC286 for each attribute). For example: If you wish to set Attribute "Service-Type" with value of "Framed", you would provide this attribute with the value of 6 (see: http://tools.ietf.org/html/rfc2865#section-5.6)

Click **Test Connection** to verify that the connection to the external system is functioning properly.

External System - SQL

You can define the SQL external System to connect to the SQL server.

The connection can be established once this external system is enabled.

SQL External System Parameters

Parameter	Description
Name	The external system's name.
Database Type	The database type.
Server IP	The IP address of the SQL server.
Port	The port number of the SQL service on the SQL server.
Server Name/Domain	Enables you to specify a specific domain name.
Database Name	Name of the Database.
User Name	The name of the user as it appears on the SQL server.
Password	The password to use when connecting to the SQL server.
Verify Pasword	Re-enter the password.

Click **Test Connection** to verify that the connection to the external system is functioning properly.

External System - SSH Proxy

If the network topology is such that the MX does not have access to the servers which it needs to scan, you can define an SSH Proxy through which the scans will be run. The MX will open an SSH session to the SSH proxy and access the scanned servers through the proxy.

The SSH proxy can be any machine, including a SecureSphere Gateway, which:

- has access to the servers to be scanned, *and*
- which the MX can access via SSH.

Once you have defined an SSH proxy, it will appear as a choice in the **Scan Proxy** dropdown menu (**Servers** tab in **Main** > **Sites** > **Server Group**).

If you want to use a SecureSphere Gateway as an SSH proxy, you still must define it here, otherwise it will not appear as one of the choices under **Scan Proxy**.

SSH Proxy External System Parameters

Parameter	Description
Enabled	Check **Enabled** if you will be running scans using this proxy.
Name	The SSH proxy's name. This name will appear in the **Scan Proxy** dropdown menu. It does not have to be the same as the proxy's hostname.
Server IP	The IP address of the SSH proxy.
User Name	The name of the user under whose account the SSH session on the proxy will be opened.
Password	The user's password.
Verify Pasword	Re-enter the password.

After entering the above parameters and clicking **Save**, you can test the connection by clicking **Test Connection**.

File URM

These parameters relate to File User Rights Management, specifically to viewing URM results.

If you change any of these parameters, click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the ***SecureSphere User Guide*.**

File URM Window Parameters

Parameter	Description
Server Request Time Limit	When viewing URM results, the number of seconds after which a query to the server will be considered as having timed out. If this happens, the user will be asked to filter the data in order to reduce the amount of data returned. **Default**: 40 seconds

Keywords Settings

These parameters allow administrators to define keywords to be used in filtering reports.

The ADC keywords in the following table are ADC pre-defined.

Keywords Settings Window Parameters

Key Name	Description
Basel II	Indicates that a report is a Basel II report. **Defaults**: **Filter Enabled** and **ADC**: selected
EBS	Indicates that a report is an EBS report. **Defaults**: **Filter Enabled** and **ADC**: selected
GLBA	Indicates that a report is a GLBA report. **Defaults**: **Filter Enabled** and **ADC**: selected
HIPAA	Indicates that a report is a HIPAA report. **Defaults**: **Filter Enabled** and **ADC**: selected
ISO 27001	Indicates that a report is an ISO 27001 report. **Defaults**: **Filter Enabled** and **ADC**: selected
PCI	Indicates that a report is a PCI report. **Defaults**: **Filter Enabled** and **ADC**: selected
PeopleSoft	Indicates that a report is a PeopleSoft report. **Defaults**: **Filter Enabled** and **ADC**: selected
Privacy	Indicates that a report is a Privacy report. **Defaults**: **Filter Enabled** and **ADC**: selected
SAP	Indicates that a report is a SAP report. **Defaults**: **Filter Enabled** and **ADC**: selected
SOX	Indicates that a report is a SOX report. **Defaults**: **Filter Enabled** and **ADC**: selected
SharePoint	Indicates that a report is a SharePoint report. **Defaults**: **Filter Enabled** and **ADC**: selected

To define a new keyword:

1. Click  .
2. Enter the keyword's **Name**.
3. If you want to able to filter the list of reports based on this keyword, select **Filter Enabled**.

   If **Filter Enabled** is not selected, then you cannot filter the list of reports by this keyword, but you can still associate the keyword with a report.

   For user-defined keywords, **ADC** is by default not selected, and this cannot be changed.
4. Click **Save**.

   If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the **SecureSphere User Guide.**

To delete a keyword:

1. Select the keyword.
2. Click  .
3. Click **Save**.

   If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the **SecureSphere User Guide**.

To associate a user-defined keyword with a report:

1. In the **Main** workspace, click **Reports** > **Manage Reports**.
2. Select a report.
3. In the **General Details** tab, move the user-defined keyword from **User Defined Keywords** to **Report Keywords**.
4. Click **Save**.

   If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the **SecureSphere User Guide.**

Log Collectors

These parameters relate to Log Collectors. Note that Log Collectors and instances of Log Collectors are defined in different parts of the SecureSphere GUI.

- Log Collectors are defined, edited and deleted in the **System Definitions** window.
- Instances of Log Collectors are defined for specific database services on specific database servers or server groups in the **Main** workspace, under **Sites**.

The following types of Log Collectors are available:

- DB2 over AS400
- Teradata (versions prior to 13.0)

Defining Log Collectors

You can create a new Log Collector, or edit and delete an existing one.

To create a new Log Collector:

1. In the **Admin** workspace, click **System Definitions**.
2. In the **System Definitions** pane, select **Log Collectors**.
3. In the **Collector Definitions** pane, click .
4. Enter the Log Collector's **Name**.
5. In the **Create Collector Definitions** window, enter the parameters.
6. Edit the Log Collector's parameters.

   See Log Collector Parameters on page 320 for an explanation of Log Collector parameters.
7. If you change any of these parameters, click **Save**.

   If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the **SecureSphere User Guide.**

To edit an existing Log Collector:

1. In the **Admin** workspace, click **System Definitions**.
2. In the **System Definitions** pane, select **Log Collectors**.
3. In the **Collector Definitions** pane, select an Log Collector from the list.
4. Expand the Log Collector by clicking on the plus-sign to the left of its name.
5. Edit the Log Collector's parameters.

   See Log Collector Parameters on page 320 for an explanation of Log Collector parameters.
6. If you change any of these parameters, click **Save**.

   If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the **SecureSphere User Guide.**

To delete an existing Log Collector:

1. In the **Admin** workspace, click **System Definitions**.
2. In the **System Definitions** pane, select **Log Collectors**.
3. In the **Collector Definitions** pane, select an Log Collector from the list.
4. Click .
5. Click **Save**.

   If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the ***SecureSphere User Guide***.

Log Collector Parameters

Log Collector Parameters

Parameter	Description
Name	The Log Collector's name.
Executable	The name of the Log Collector executable file.
Supported Services	The database service's supported by the Log Collector.
Supported Protocols	The protocols supported by the Log Collector.
User	The user name with which the Log Collector logs on to the database.
Password	The password.
Location	Additional information required to specify the location of the logs on the Host. For example, directory (for FTP and SCP), or the URL (for HTTP and HTTPS) or the database schema.
Delete Log	Enable **Delete Processed Log** to delete logs (on the database server) which have been converted to CSV format and sent to the SecureSphere gateway process.
Additional Configuration	Additional parameters defining the Log Collector. Contact Imperva support before changing these.
Additional Configuration Template	The name of a file containing additional configuration information. Click **Upload File** to obtain this file.
Additional Configuration XML Validation	The name of a file containing additional configuration information relating to XML validation. Click **Upload File** to obtain this file.

Lookup Data

These parameters are related to lookup data. For more information, see Protecting and Auditing Custom Information with Lookup Data on page 362.

If you change this parameter, click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the ***SecureSphere User Guide***.

Lookup Data Window Parameters

Parameter	Description
Query Timeout	Determines the period of time after which no reponse is received that the query shall time out. **Default: 15 minutes**
Maximal Lookup Data Set Size	Maximum Lookup Dataset size, that is, the maximum number of results returned from the query. Lookup Dataset size is defined in **Main** > **Setup** > **Global Objects**. **Default**: 10000

Policy Settings

These parameters relate to Security Policies.

If you change any of these parameters, click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the ***SecureSphere User Guide***.

Policy Settings Window Parameters

Parameter	Description
Enable comments for policy changes	If enabled, users are able to add comments when modifying a Security Policy. **Default**: Disabled

Report Settings

These parameters are related to reports.

If you change any of these parameters, click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the ***SecureSphere User Guide***.

Report Settings Window Parameters

Parameter	Description
Maximal number of rows in a report in CSV format	The maximum number of rows in a CSV format report. Additional data beyond this number of rows will not be included in the report. **Default**: 10000
Enable the downloading of additional fonts when working with different languages.	If checked, SecureSphere assumes that all PDF reports include East Asian fonts, and requires that the user install these fonts before viewing PDF reports. If not checked, SecureSphere assumes that PDF reports do not include East Asian fonts, so if a report does include these fonts it will be incorrectly displayed.
Maximal number of pages in a report in PDF format	The maximum number of pages in a PDF format report. Additional data beyond this number of pages will not be included in the report. **Default**: 500

Report Settings Window Parameters (continued)

Parameter	Description
Template for results files	A sequence of placeholders which defines the report's file name. **Default**: ${reportName}_${username}_${date}
Include report sent by e-mail followed action as link instead of attachment	Include a direct link to a report when an e-mail followed action is used. When disabled, the report is sent as an attachment. **Default**: Disabled.
URL for reports and tasks links	The URL of SecureSphere which hosts reports, for example https://10.3.250.103:8083. SecureSphere then appends the URL so that it directs users to the specific report. **Default**: The default SecureSphere Management Server IP address.

Server Definitions

These parameters relate to the MX server.

Server Definition Window Parameters

Parameter	Description
Server Name	You can assign a name to the Management Server. This name will be displayed in the title of the SecureSphere GUI window. This name can be different from the MX appliance's hostname. **Default**: none

Stored Procedures Settings

These parameters define how name conflicts are resolved and empty stored procedures saved when importing stored procedures.

If you change any of these parameters, click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the ***SecureSphere User Guide***.

Stored Procedures Settings Window Parameters

Parameter	Description
Override existing built in stored procedure data	If selected, imported built-in stored procedures replace existing built-in stored procedures with the same name. **Default**: selected
Override existing user defined stored procedure data	If selected, imported user-defined stored procedures replace existing user-defined stored procedures with the same name. **Default**: selected
Save empty built in stored procedures	Empty built-in stored procedures are saved in the SecureSphere database. **Default**: not selected

Stored Procedures Settings Window Parameters (continued)

Parameter	Description
Save empty user defined stored procedures	Empty user-defined stored procedures imported from the database are saved in the SecureSphere database. **Default**: not selected



Note: Built-in stored procedures are those provided by the database vendor.

System Events Notifications

These parameters relate to system event notifications.

If you change any of these parameters, click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the ***SecureSphere User Guide***.

System Events Notifications Settings Window Parameters

Parameter	Description
Gaps in minutes between consecutive gateway overload messages	When a gateway cannot process all the traffic, a system event is generated as a warning. Another system event is created if the gateway is still overloaded after this interval. **Default**: 15 minutes
Gap in minutes between consecutive ambiguous packets messages	Generate an ambiguous packet message only if this interval has passed since the last such message. **Default**: 5 minutes
Issue a system event when a gateway blocks more than the following number of ambiguous packets per minute	Generate a system event if the gateway blocks more than this number of packets in one minute. **Default**: 60 packets
Issue a system event when the following CPU utilization percentage is exceeded	Generate a system event if CPU utilization exceeds this percentage. **Default**: 90 percent
Gap in minutes between consecutive CPU utilization messages	Generate a CPU utilization system event only if this interval has passed since the last CPU utilization system event was generated. **Default**: 60 minutes
Gap in minutes between consecutive gateway throughput messages	Generate a gateway throughput system event only if this interval has passed since the last gateway throughput system event was generated. **Default**: 60 minutes
Issue a system event when the following throughput is exceeded	Generate a system event if the gateway throughput exceeds this rate. **Default**: 90 MBs / second
Issue a system event when the ADC content has not been updated for the following number of days	Generate a system event if this interval has passed since ADC content was updated. **Default**: 30 days

User Interface Settings

This section describes the windows related to the user interface (GUI), and includes:

Display Limits on page 325
Language Settings on page 325

Display Limits

These parameters relate to the display of items in the SecureSphere GUI.

If you change any of these parameters, click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the ***SecureSphere User Guide***.

Display Limits Window Parameters

Parameter	Description
Maximum options in pushdown menu	The maximum number of items displayed in drop-down menus. If the list includes more items, they are not displayed and are not available for selection. **Default**: 500 items
Maximum rows in table	The maximum number of items displayed in tables. If the list includes more items, they are not displayed and are not available for editing. **Default**: 500 item

Language Settings

These parameters define the language used in the SecureSphere GUI.

If you change this parameter, click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the ***SecureSphere User Guide***.

Language Settings Window Parameters

Parameter	Description
Select Display Language	The language in which GUI elements will be displayed. **Default**: English
Change language without affecting the database	If enabled, texts in the SecureSphere database, for example, policy names, will not be translated into the **Display Language** when displayed in the GUI. **Default**: Enabled

ThreatRadar Settings

This section describes the windows related to ThreatRadar, and includes:

General Settings on page 326

General Settings

This parameter enables you to enable or disable ThreatRadar.

If you change this parameter, click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the ***SecureSphere User Guide***.

General Settings Window Parameters

Parameter	Description
ThreatRadara is Enabled	If enabled, SecureSphere ThreatRadar is enabled. **Default**: not selected

Miscellaneous Audit Data Operations

The following procedures are used to configure various aspects of audit operations:

- Changing the Audit Directory Path on page 327
- Configuring Encryption on page 328

Changing the Audit Directory Path

The audit directory path in SecureSphere is configured by default under **`var/SecureSphere/audit`**. This path can be changed when wanting to store audit data in a different location than the default, including on an external volume.

To change the audit directory path:

1. SSH to the SecureSphere gateway (or Onebox in onebox configurations) using the credentials configured by the administrator during SecureSphere installation.
2. Create a mount point and mount the storage drive for the new location.
3. Navigate to the directory containing the **`boostrap.xml`** file by using the following command (default location):

```
cd /opt/SecureSphere/etc
```

4. Open the **`bootstrap.xml`** file using a text editor.
5. Modify the audit default settings whose location is indicated in the following:

```
<auditor-default-settings max-records-per-file="1000000"
max-file-size="512000000" max-saved-files="1095" max-aggregated-
records="10000" min-free-disk-space="2000000000"
min-free-disk-space-percent="10" low-free-disk-space="4000000000"
low-free-disk-space-percent="15"
audit-base-path="/var/SecureSphere"
use-audit-thread="true" max-records-per-time-slot="10000"/>
```

6. Save the changes and close the text editor.
7. Restart the gateway. Changes only take effect once restart has been completed.
8. If you already have existing audit data on SecureSphere, you must do one of the following:
   - **To keep existing data**: Move all data including directories and files from the old directory to the new directory.
   - **To purge existing data from the management server**: Delete data from old directory, and cleanup Fast View data from the management server database by clicking **Apply** under **Alert Management Statistics** > **Management Server View** > **Apply**.

Configuring Encryption

You can configure SecureSphere to encrypt audit data located on the gateway hard disk. Configuring encryption includes activating encryption on each gateway, which will then manage encryption and decryption of all data on that gateway, then restarting the gateway in order for encryption to take effect. By default, encryption is turned off.



Notes:

- Turning encryption on and off does not cause loss of data already collected.
- Enabling encryption can impact system performance.
- Data that was already on the gateway and not previously encrypted remains unencrypted even if encryption is enabled.

To configure encryption:

1. Login to the management server with the user: `root`
2. Execute the following command:

```
impctl gateway config --encryption=T
```



Note: To disable configuration, execute: impctl gateway config --encryption=F

3. Restart the gateway by executing the following command:

```
impctl gateway restart
```

CHAPTER 15

System Performance

This chapter describes the **System Performance** window, which displays performance data about management servers, gateways and remote agents.

Management Server on page 330

Gateways and Agents on page 333

Troubleshooting Performance on page 335

Management Server

The **Management Server** window displays real-time information about the management server.

To display real-time information about the management server:

1. In the **Admin** workspace, click **System Performance**.
2. In the **System Performance** pane on the left, click **Management Server.**

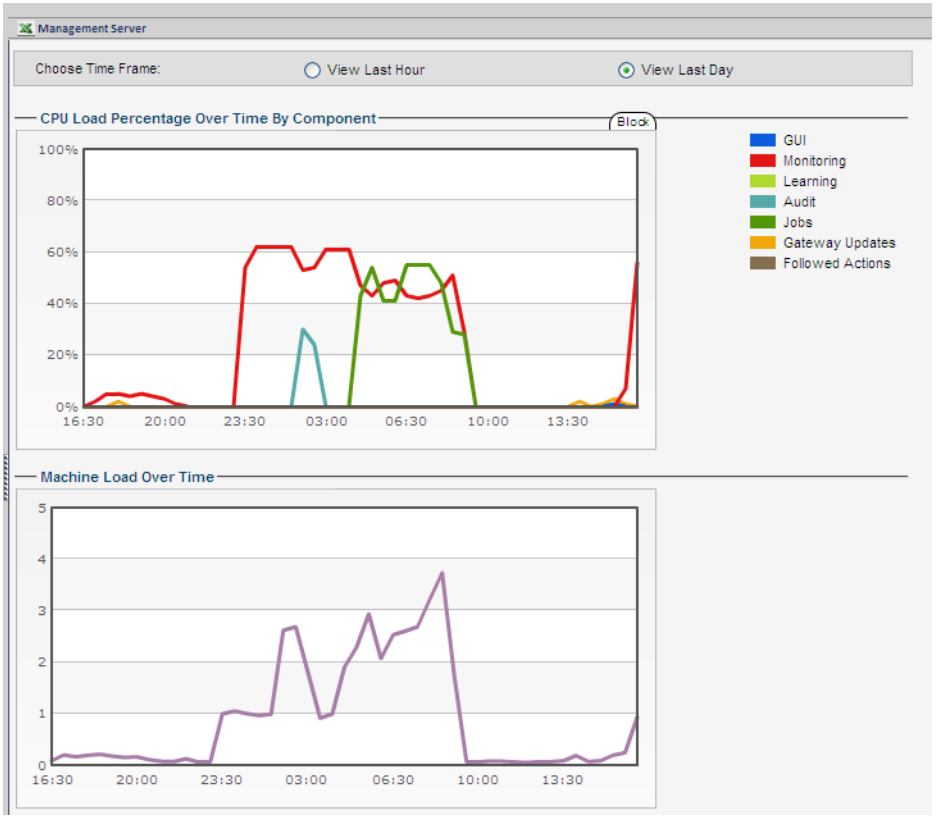


Figure 62 System Maintenance - Management Server

If the management server is in an MX-HA configuration, the IP address of the active server is displayed at the top of the window.

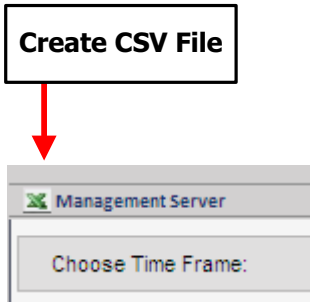
The graphs display the following information:

Graph	Displays
CPU Load Percentage Over Time By Component	The CPU load attributable to each of the management server's functions. Each line is differently colored and represents a different function, according to the color-coded list of functions alongside the graph. **Note:** The **Jobs** graph displays only jobs whose CPU usage is greater than 10%.
Machine Load Over Time	The overall machine load over time, as returned by the Linux "top" command.

3. You can change the time period displayed in the graphs by selecting **View Last Hour** or **View Last Day**.

4. To output the data in the graphs to a CSV file:

   4.1 Click  (to the left of the words **Management Server** at the top of the window).



   4.2 Alternatively, you can click **Save As** (in the upper right corner) and select **Save as CSV**.



   4.3 To move the generation of the CSV file to a background process, click **Move to Background** in the **Export CSV window**.

   The data in the CSV file is the same data displayed in the graphs.



Note: The exported data relate to the previous 24 hours.

Exporting Technical Information from Management Servers

On occassion, when encountering trouble with SecureSphere operation, Imperva support may request that you provide them with technical information that is automatically generated by SecureSphere, so they can analyze logs and other information. You can export this information from the SecureSphere Management Server using the GUI. This procedure describes how to export technical information for a SecureSphere Management Server from the GUI. For information on exporting technical information from SecureSphere gateways or Onebox architectures, see Exporting Technical Information from Gateway and Onebox on page 219.

To export technical information from Management Servers:

1. In the **Admin** workspace, select **System Performance** > **Management Server.**
2. From the top of the **Details** pane, click **MX Tech Info**.

   SecureSphere prepares the information for download. Once complete a dialog box appears with a link. Click the link and download the zip file to the desired location. You can then mail it to Imperva support for analysis.



Note: When exporting technical information from a Onebox architecture, both Gateway and Management Server technical information is exported.

Gateways and Agents

The **Gateways and Agents** window displays real-time information about the gateways and DB Agents.

To display real-time information about gateways and DB Agents:

1. In the **Admin** workspace, click **System Performance**.
2. In the **System Performance** pane on the left, click **Gateways & Agents.**



Note: data are displayed only for those gateways for which **Enable** is checked under **Performance Profiling** in the **Gateway Group Details** window (see Gateway Groups on page 215).

3. Select a time period:
   - **Last 24 hours**:
   - **Last Hour**:
   - **Custom**: If you choose **Custom**, you will be asked to define a custom time frame (between **From Date and Time** and **To Date and Time**) and to click **Set**.

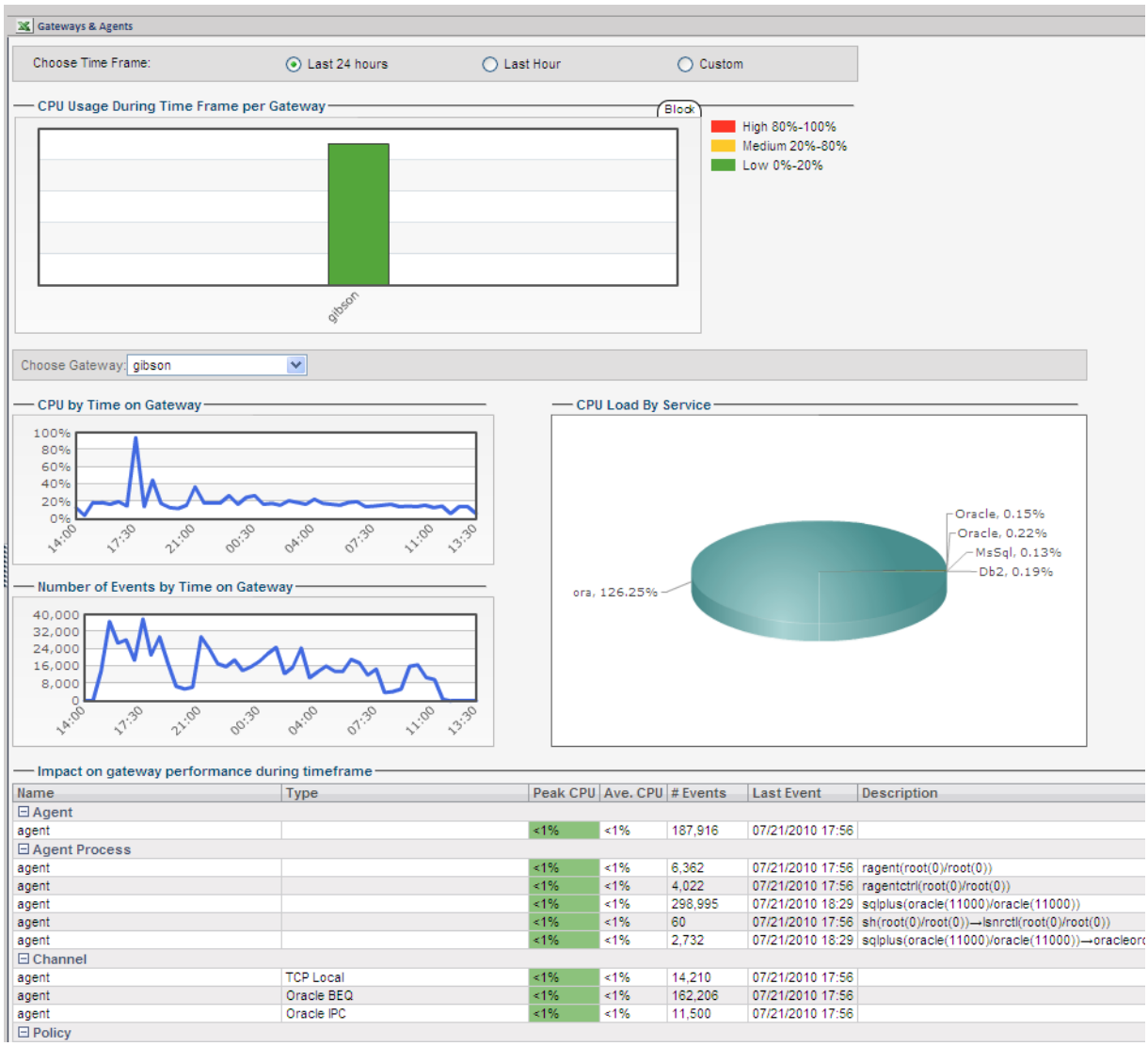


Figure 63 System Maintenance - Gateways and DB Agents

This window is divided into several sections, and displays the following information about the selected time period:

- **CPU Usage During Timeframe per Gateway** - The CPU usage for each gateway during the selected time period.

4. **Choose Gateway** - Select a gateway from the list.

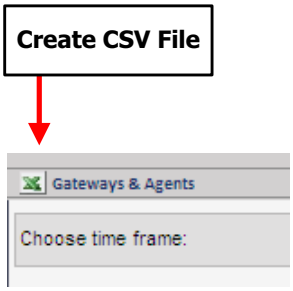
Note: An event occurs when SecureSphere "hooks into" the traffic stream, for example, to parse it.

The following information is displayed about the selected gateway:

Section	Displays
CPU / # of Events by Time on Gateway	The graph at the top displays the percentage of CPU use by events. The bottom graph displays the number of events over time.
CPU Load By Service	This pie chart shows the distribution of events by site-server group-service.
Impact on gateway performance during timeframe	The events table groups events of the last 72 hours by time and displays the resources used by each type of event. You can expand the event types to view sub-groups of events. **Note:** Agent process details refer to the process on the server monitored by the DB Agent.

5. You can change the time period displayed in the graphs by selecting **Last 24 Hours** or **Last Hour** or **Custom**.
6. To output the data in the graphs to a CSV file:

6.1 Click  (to the left of the words **Gateways & Agents** at the top of the window).



6.2 Alternatively, you can click **Save As** (in the upper right corner) and select **Save as CSV**.



6.3 To move the generation of the CSV file to a background process, click **Move to Background** in the **Export CSV window**.

Note: The exported data relate to the previous 72 hours.

Troubleshooting Performance

By periodically reviewing the **System Performance** data, you can identify bottlenecks and other problems in your SecureSphere deployment. Some guidelines are given below.

The following topics are described:

Management Server on page 335
Gateways and Agents on page 335

Management Server

If your management server's performance seems excessive over a long time frame, identify the components that use the most CPU resources. Peaks in CPU usage are common and are to be expected, so you should investigate only consistent and prolonged high CPU usage.

Bear in mind that high CPU usage indicate nothing more than high traffic, so review the CPU usage at irregular intervals to determine whether there really is a problem or not.

Component showing consistently high CPU usage	
GUI	It may be that too many users are connected to the GUI at the same time.
Monitoring	You should tune alerts.
Learning	Implement gradual learning.
Audit	It may be that you are trying to view too much audit data at the same time. Consider creating custom time frames that implement the fast view capabilities.
Jobs	These include reports, assessments, scans, archive, Active Modules, Lookup Data sets imports and purges. Consider scheduling these jobs to distribute the load evenly during the day/week. Alternatively, review the jobs to confirm that they are running on relevant data.
Gateway Updates	It may be that one or more of the gateways is repeatedly requesting configuration. Look for errors in **Setup** > **Gateways**.
Followed Actions	These include emails, syslog actions, archive storage, SNMP and OS commands. Some of these may be CPU intensive because of file size or errors. Review the followed actions and identify these problems.

The values on the vertical scale of the **Machine Load Over Time** graph are the "processes" values returned by the Linux "top" command, defined as follows:

> The total number of processes running at the time of the last update. This is also broken down into the number of tasks which are running, sleeping, stopped, or undead. The processes and states display may be toggled by the t interactive command.

Gateways and Agents

This window summarizes the resource usage of various SecureSphere components on a specific gateway.

The following topics are described:

System Performance - CPU Load on page 336
System Performance - Policies on page 336

System Performance - Signature and Dictionaries on page 336
System Performance - SSL on page 336
System Performance - Agents on page 336

System Performance - CPU Load

If the CPU usage for a specific gateway seems excessive over a long time frame, identify peak periods of CPU usage, narrowing the time frame.

In the **CPU Load By Service** graph, you can identify the services that incur the highest CPU loads. For each of these services, review the policies, signatures and dictionaries associated with the service to determine which of these might be responsible.

You may find, after investigation, that you need an additional gateway, or that the gateway needs to be upgraded to a more powerful model.

System Performance - Policies

For each service with a high CPU load, review the following:

- Identify the alerts that match the policy and rule of this service. If these are false positives, fine tune the policy or unapply it from the application(s), service(s) or server group(s) where the false positives occurred.

  Consider also the possibility that the policy is not required.
- If an audit policy uses too much CPU, it may be too complex. The problem may also be that the relevant signatures and dictionaries are CPU-intensive (see System Performance - Signature and Dictionaries below).
- Alternatively, edit the policy by changing some of the criteria or unapply it from some services.

System Performance - Signature and Dictionaries

For each service with a high CPU load, review the following:

Component	Description
Security Signatures	Review the signature (**Main** > **Setup** > **Signatures**) and determine whether it can be safely disabled (ADC signatures) or modified (custom signatures).
SQL Dictionaries (including Stored Procedures & Privileged Operations)	In **Main** > **Setup** > **Global Objects**, review stored procedures and privileged operations and disable those which are not required.
Generic Dictionaries (including Sensitive Data Dictionaries)	Identify the policies using the dictionary, and edit or unapply them accordingly.
SQL injection / XSS	In **Monitor** > **Alerts**, review the most frequently-occurring SSL injection and XSS alerts, and create exceptions for those which are false positives.

System Performance - SSL

If SSL operations are consuming significant CPU resources, consider installing an SSL accelerator.

Alternatively, configure the Web server to reuse SSL sessions.

System Performance - Agents

DB agents run on the DB server and communicate with a SecureSphere gateway, so they use resources on both machines.

On the DB Server

In **Main** > **Setup** > **Agents**, you can see the CPU usage and other statistics for each agent in the **General Details** tab. If an agent's CPU usage is excessive, then use OS platform commands to determine which agent process is responsible. Sometimes excessive CPU usage is reflected in the gateway's statistics (see On the Gateway below).

Review the relevant audit policies. It may be that it is not necessary to audit all of the database traffic, in which case you should create appropriate exclusions.

Otherwise, you may be able to reduce the CPU load by reconfiguring the deployment.

On the Gateway

In the **Impact on gateway performance during timeframe** table, you can see the CPU resources consumed by each DB Agent communicating with the gateway. Excessive CPU usage on the gateway may indicate a problem with the DB Agent, for example, if the DB Agent is monitoring a backup process. In this case you should create an exclusion on the DB Agent.

CHAPTER 16

Gateway High Availability

The term “High Availability” refers to SecureSphere’s ability to maintain connectivity and monitoring even when a SecureSphere appliance fails.



Note: Two gateways in a High Availability deployment must be configured identically (same policies, objects, *etc.*)

This chapter describes the High Availability options for deploying SecureSphere, and includes:

- Layer 2 High Availability Deployments on page 340
- Layer 3 (Proxy) High Availability Deployments on page 344
- Other High Availability Deployments on page 346

Layer 2 High Availability Deployments

It is possible to deploy High Availability at layer 2 as follows:

- At the Network Level on page 340
- At the SecureSphere Level on page 340

At the Network Level

Examples of layer 2 High Availability deployments at the network level include:

- Link Aggregation (Etherchannel) on page 340
- RSTP (Rapid Spanning Tree Protocol)

Link Aggregation (Etherchannel)

One or more SecureSphere gateways can support link aggregation. For example, two interfaces on a SecureSphere gateway can be connected to two interfaces on a network load balancer. Traffic can pass through both connections. For example, uplink traffic can travel through the first interface card while downlink traffic goes through the second interface card.

In bridge mode, each SecureSphere gateway includes four network interfaces dedicated to application security. So it is possible to aggregate traffic through two connections. If the load balancer has 100Mbps Fast Ethernet interfaces, then aggregating links can also increase total throughput. Even if the traffic is split between the two segments, SecureSphere can accurately inspect all traffic and block attacks.

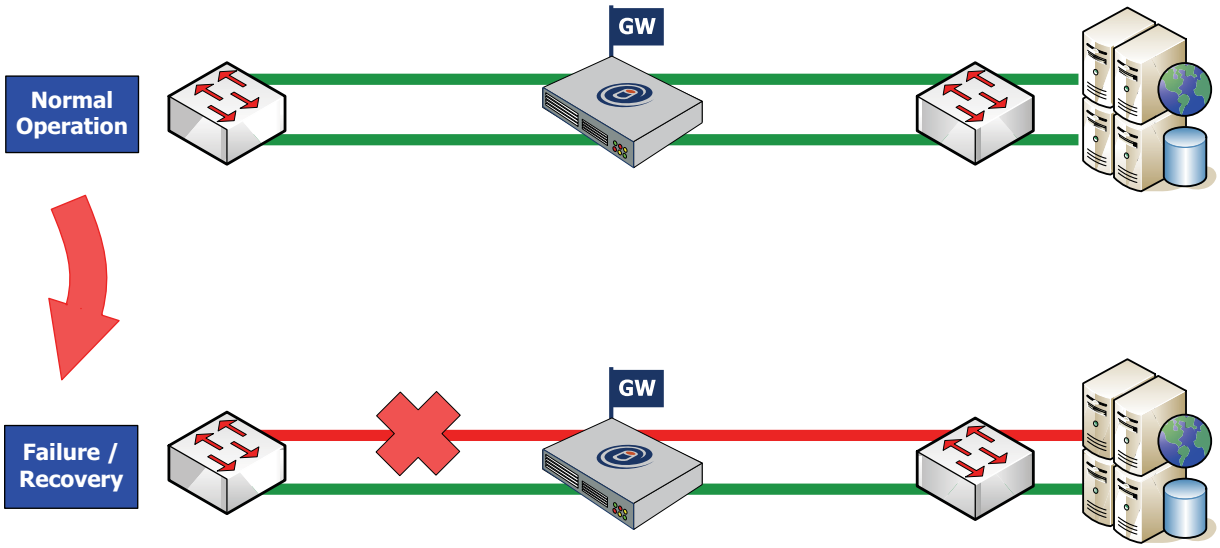


Figure 64 Link Aggregation

If an Ethernet cable is disconnected or a network interface fails, then traffic will continue to be forwarded through the active link on the SecureSphere gateway.

At the SecureSphere Level

Examples of layer 2 High Availability deployments at the SecureSphere level include:

- IMPVHA Protocol — Active-Passive and Active-Active Failover on page 341
- Bridge STP on page 341

IMPVHA Protocol — Active-Passive and Active-Active Failover

IMPVHA is a proprietary redundancy protocol developed by Imperva for environments which do not have a redundant network architecture and STP cannot be implemented. For some environments, STP convergence times may be unacceptably long or STP may conflict with existing protocols, such as RSTP. In these situations, the Imperva High Availability (IMPVHA) protocol is the ideal solution.

With IMPVHA, two SecureSphere gateways can be configured as layer 2 bridges in either active-passive or active-active mode. The configuration and failover mechanism is similar to VRRP, except that when a failover occurs, the backup device informs connected devices to redirect traffic via ARP requests rather than assuming the primary device's IP address. When an IMPVHA pair is deployed, the backup gateway sends periodic loopcheck broadcast messages. If no response is received within the configurable failover time (default is 0.5 seconds), the backup gateway becomes active.

Since a SecureSphere gateway supports two bridges through its four network interface cards, it is possible to configure one bridge as the IMPVHA primary for one network and the second bridge as a backup for another network. In this configuration, two SecureSphere gateways can support an active-active failover configuration.

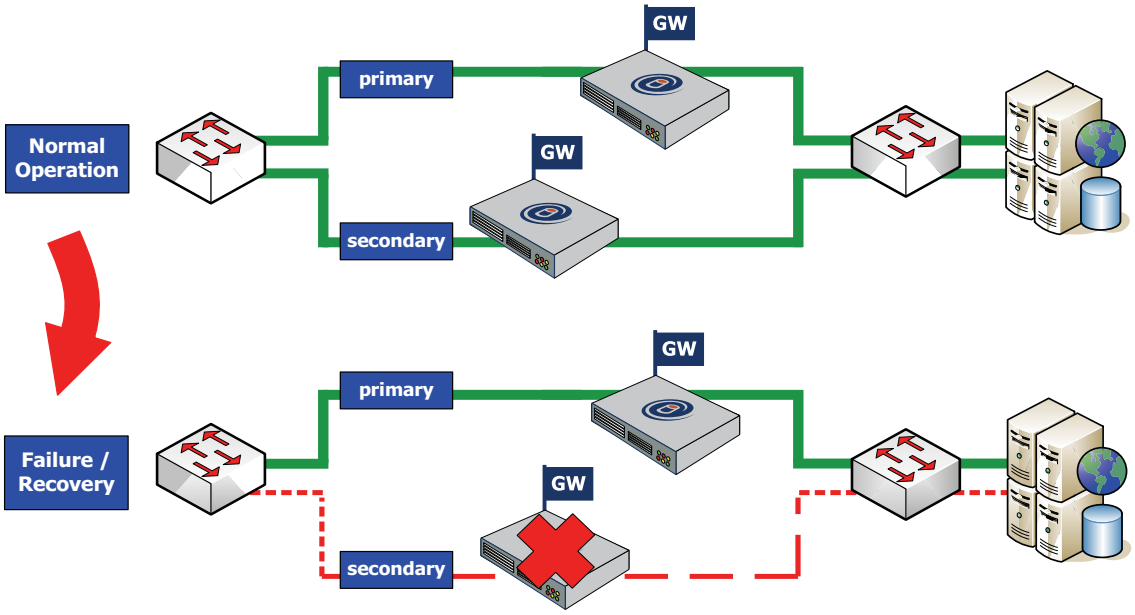


Figure 65 IMPVHA

IMPVHA — Configuration

IMPVHA is configured for each SecureSphere gateway using the `impcfg` command line utility. Configure each gateway as Bridge IMPVHA with IMPVHA on.

For more information, see Configuring a Gateway as a Bridge on page 73.

Bridge STP

SecureSphere can be deployed in bridge mode in existing high-availability deployments, for example, STP. One of the SecureSphere gateways is designated as the master and the other as its backup. Initially, the network directs traffic destined for the server to the master.

If the master gateway fails, the failure appears to the network as a failure of a switch port. Connected devices automatically recognize that the failed gateway is no longer reachable and then redirect traffic to the backup gateway, which becomes the new master gateway.

If the previous master is restarted, it becomes the backup.

Because the two SecureSphere gateways are deployed as bridges (that is, they have the same policies and the SecureSphere management server sees them as two active gateways), TCP connections are negotiated

directly between the client and the back-end server. A failover event does not disrupt TCP connections or affect user sessions.

For more information, see Chapter 4, Configuring SecureSphere.

Bridge STP — Active-Passive Failover

In this deployment, only the SecureSphere gateway configured as the master is active. The backup SecureSphere gateway is in standby mode, waiting to take over if the first SecureSphere gateway fails.

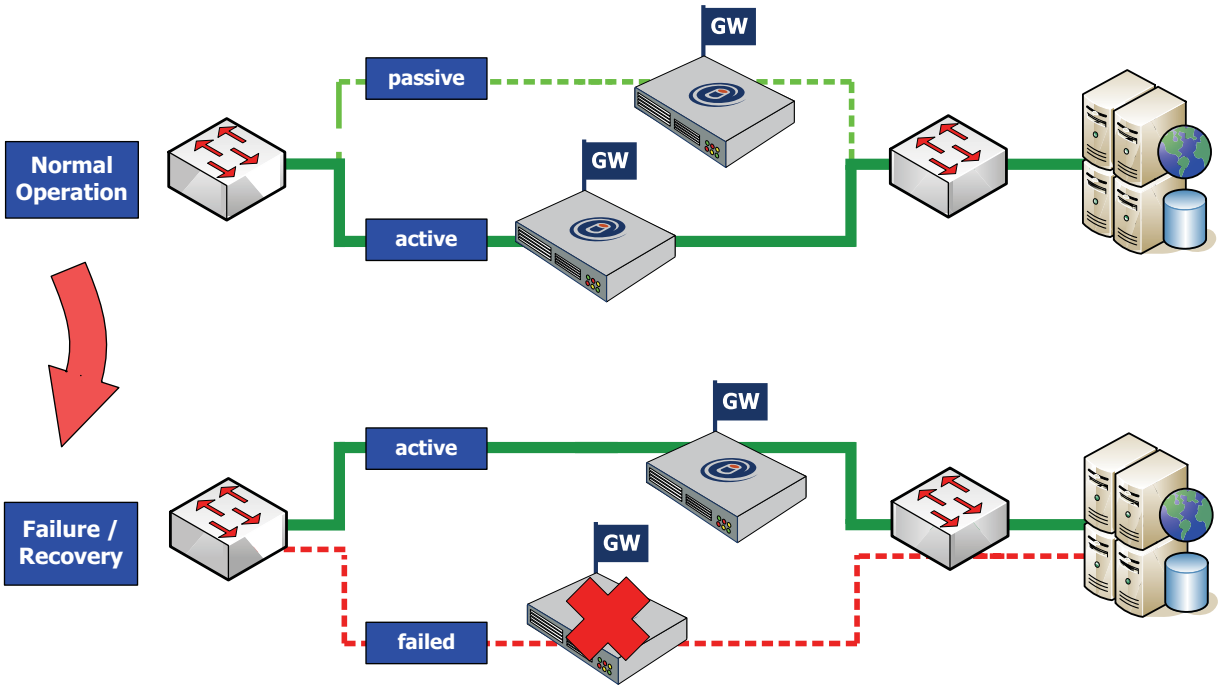


Figure 66 Active-Passive Failover

This deployment is somewhat inefficient because at any given time, one of the SecureSphere gateways is idle — it is functioning properly but is not processing any traffic.

This deployment can also be used with both transparent and non-transparent reverse proxies.

Bridge STP — Active-Active Failover

This deployment is the same as the previous one, except that both SecureSphere gateways are active and monitor traffic simultaneously. If one of them fails, all traffic flows through the other gateway. Total network capacity is reduced until the failure is corrected.

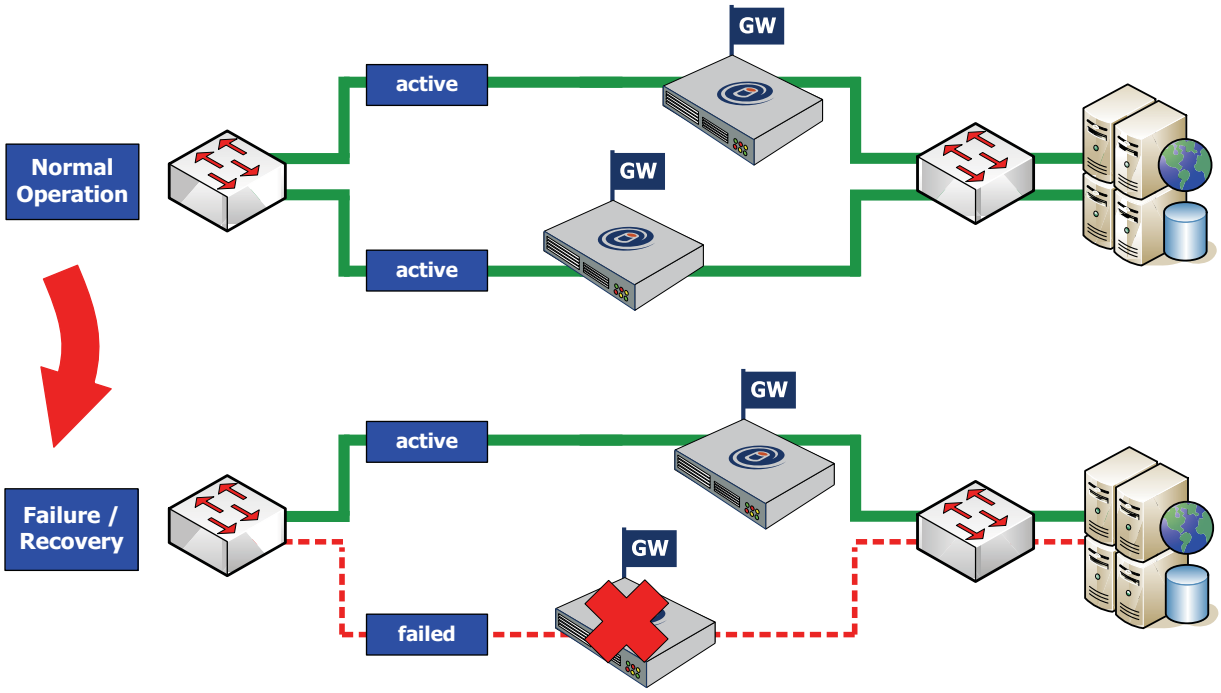


Figure 67 Active-Active Failover

This deployment supports load sharing if sessions are sticky, that is, the same session always passes through the same gateway.

When configuring such a solution, ensure that each gateway is able to handle the bandwidth of both gateways, should one of them fail.

Redundant Architecture (STP) — Configuration

If STP or a similar capability is available in the network, configure the gateways (with **`impcfg`**) as either:

- Bridge IMPVHA with IMPVHA off
- Bridge STP with STP on

For more information, see Chapter 4, Configuring SecureSphere.

Layer 3 (Proxy) High Availability Deployments

It is possible to deploy High Availability at layer 3 as follows:

- At the Network Level on page 344
- At the SecureSphere Level on page 345



Note: Proxy deployments are relevant for Web traffic only. For more information, see Chapter 2, Topologies and Deployment.

At the Network Level

SecureSphere is often deployed as a direct replacement for legacy reverse proxy appliances. In many cases, administrators choose to configure SecureSphere as a bridge because it fits into the existing architecture and reduces the operational burden associated with Web proxies. However, in some cases, administrators deploy SecureSphere as in proxy mode to meet architectural requirements or for content modification.

The SecureSphere Web Application Firewall supports both reverse proxy and transparent proxy configurations. Both proxy configurations offer content modification, including cookie signing and URL rewriting. Transparent proxy mode enables transparent deployment without network or DNS changes.

Examples of layer 3 High Availability deployments at the network level include:

- Load Balancer Integration on page 344

Load Balancer Integration

In proxy mode, one or more SecureSphere gateways are deployed as either a Reverse Proxy or a Transparent Reverse Proxy. A load balancer balances the traffic between the gateways and the gateways forward the traffic to the Web servers. It is possible to configure load balancer to work in active-active or active-passive modes.

In this mode, the IP address of the Web site resolves to the SecureSphere gateway's IP address. If SSL is used, then the gateway should be configured to terminate the SSL connection. Note that in proxy mode, SecureSphere establishes a new connection to the Web server on behalf of the client.

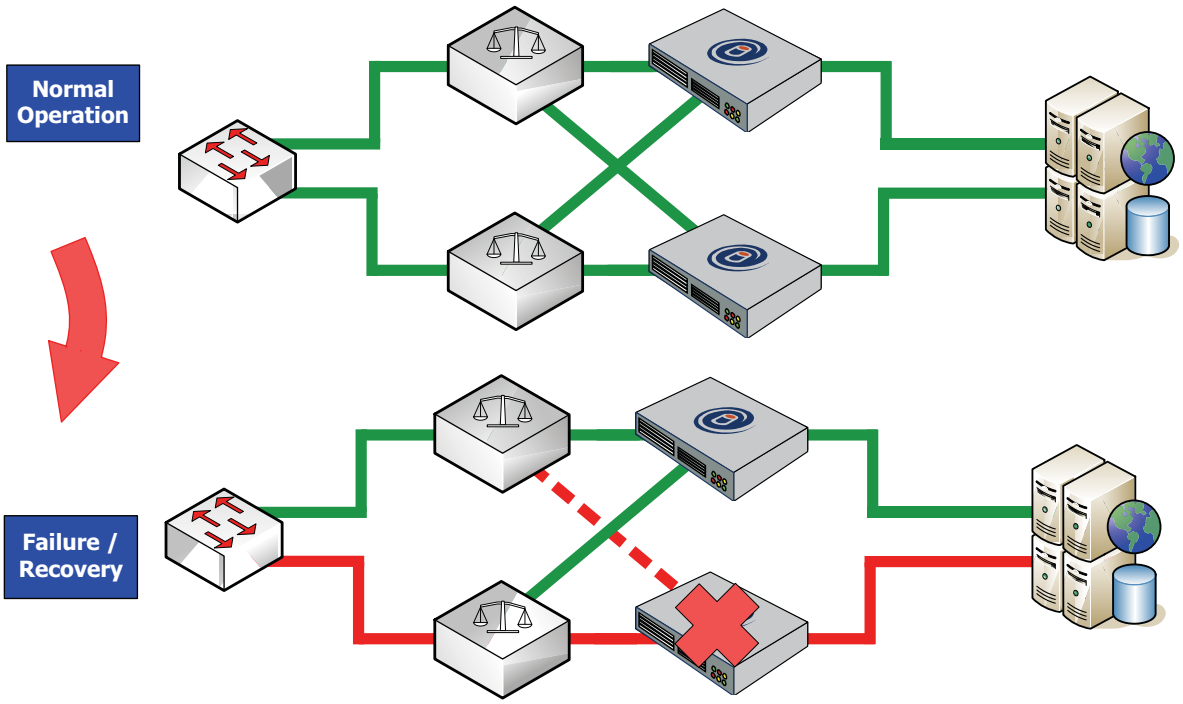


Figure 68 Load Balancer Integration

At the SecureSphere Level

Examples of layer 3 High Availability deployments at the SecureSphere level include:

- Redundant Architecture (VRRP) — Configuration on page 345

Redundant Architecture (VRRP) — Configuration

VRRP is suitable for a deployment where the SecureSphere gateway has an IP address, that is, it is not configured as a bridge or as a transparent reverse proxy, but as one of the following:

- a non-transparent reverse proxy
- a listener for DB Agents

To configure a SecureSphere gateway for VRRP, configure the aliases as virtual. For more information, see Configuring Aliases on page 105.

Other High Availability Deployments

Other High Availability deployments include:

- Fail-Open Bridge on page 346
- Sniffing Gateway High Availability on page 346

Fail-Open Bridge

Fail-open configuration preserves uptime without the cost or management effort of building and maintaining a redundant architecture. In the event of an appliance failure, SecureSphere's specialized network interface card detects the failure and physically completes the connection through the SecureSphere gateway. The NIC card will fail open in milliseconds, minimizing network downtime.

Though connectivity is maintained, application servers will not be monitored or protected from attacks until the SecureSphere gateway resumes operations.

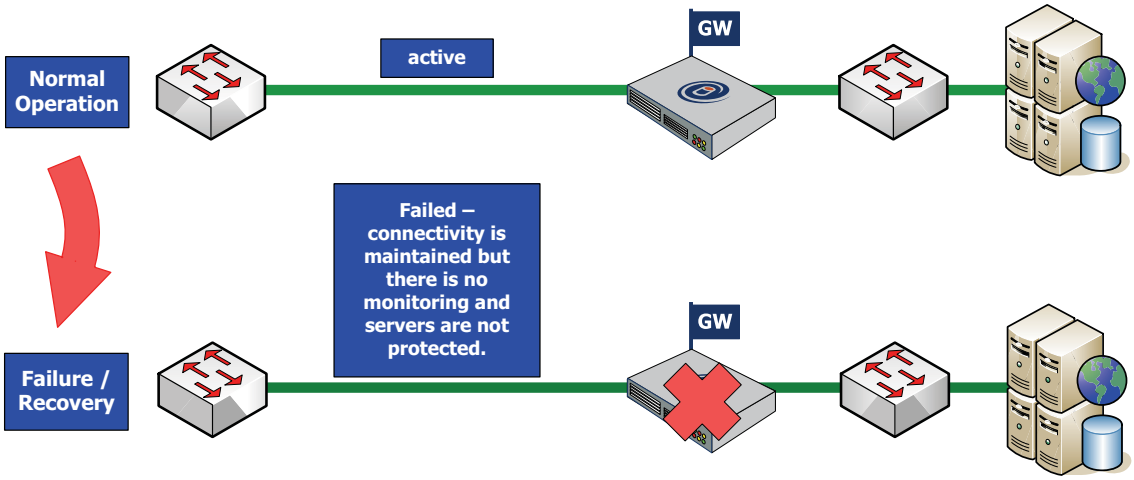


Figure 69 Fail Open Bridge

Note: A SecureSphere gateway deployed in sniffing mode provides a similar level of connectivity continuity in the event of failure: traffic continues to flow through the network but it is not monitored.

Fail Open — Configuration

The Gateway appliance is configured as fail open by default. When you first connect the Gateway appliance to the network, no sites or server groups are defined, so no policies are implemented, nothing is monitored or blocked, and all traffic is passed through the appliance.

You can change the mode using the **`impctl`** command line utility. For more information, see Chapter 4, Configuring SecureSphere.

Sniffing Gateway High Availability

Configuring SecureSphere as a sniffing gateway enables organizations to protect critical servers without introducing a new point of failure. It is a lower price alternative to deploying two or more redundant SecureSphere gateways.

To deploy SecureSphere as a sniffing gateway, connect it to an open SPAN port or a network TAP to observe traffic. A second connection to an active port on the switch allows SecureSphere to block malicious connections by sending TCP resets to the server.

In the event of a SecureSphere gateway failure, network traffic is unaffected, but it will not be monitored or protected until the SecureSphere gateway becomes operational again.

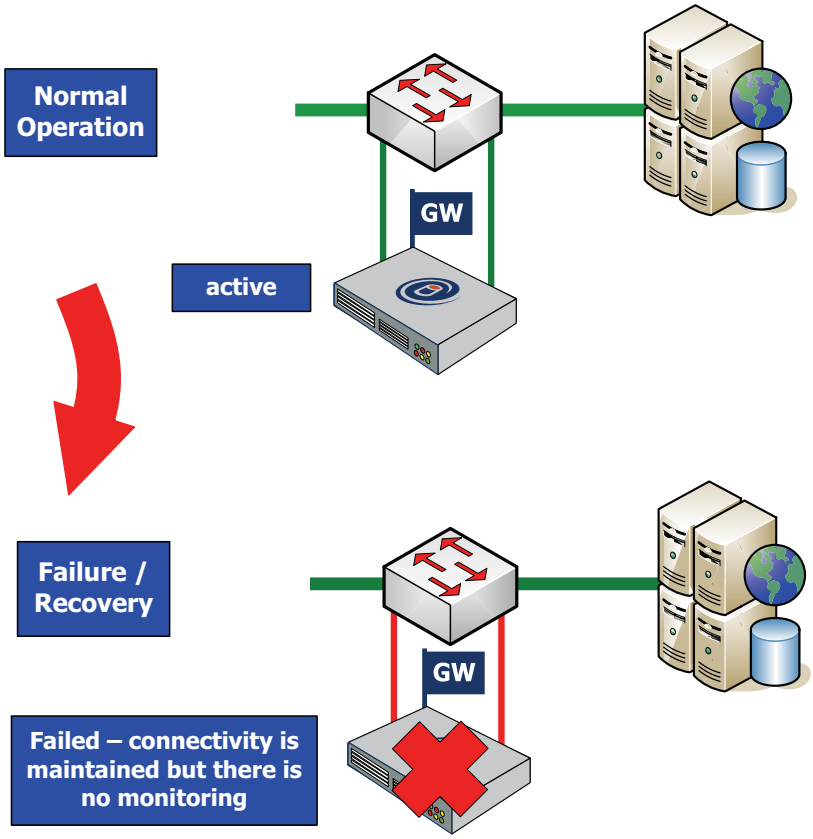


Figure 70 Network Monitor - No HA

For some organizations, it may be imperative to monitor and audit all Web or database traffic without disruption. These organizations can deploy multiple SecureSphere gateways in non-inline mode. If one of the gateways fail, the other gateway will continue to monitor and record traffic.

In this configuration, each gateway should be managed by a separate management server or by using the integrated software management option (Onebox).

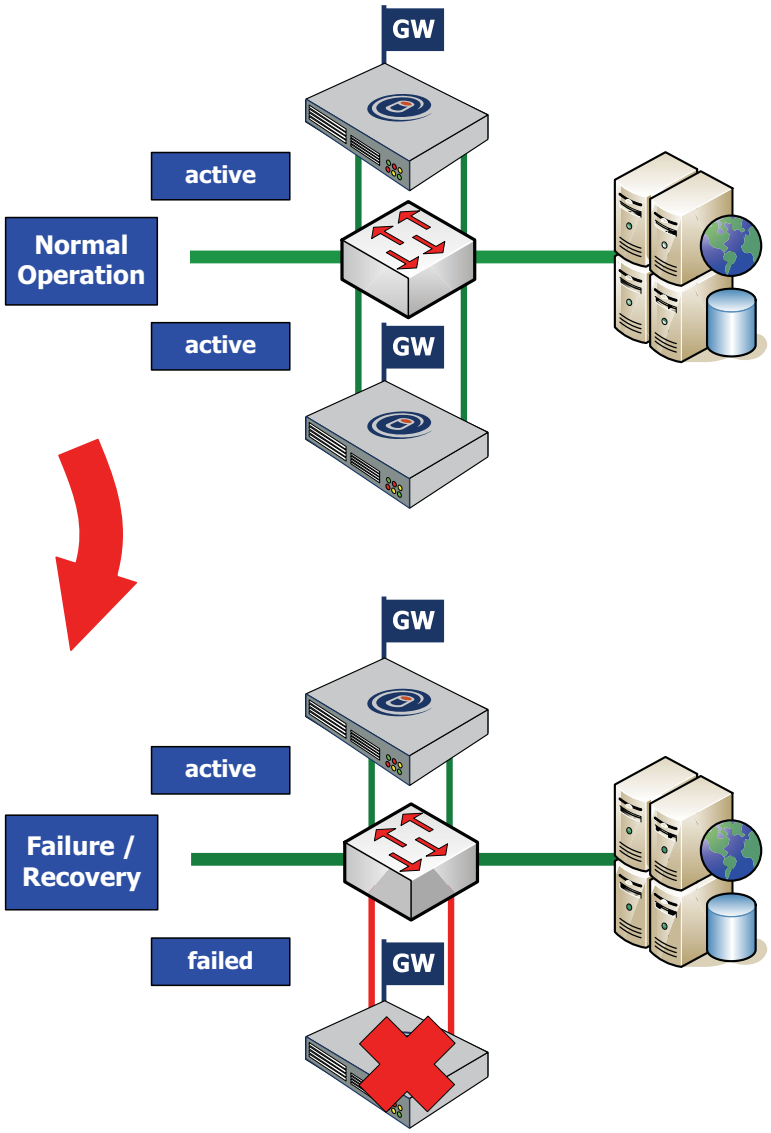


Figure 71 Sniffing - Redundant Gateways

CHAPTER 17

Management Server High Availability (MX-HA)

This chapter describes High Availability options for SecureSphere management servers, and includes:

- Management Service-High Availability (MX-HA) Overview on page 350
- Management Server-High Availability (MX-HA) Implementation on page 351
- Management Server High Availability (MX-HA) Components on page 352
- Before Installing Management Server High Availability (MX-HA) on page 353
- Installing Management Server High Availability (MX-HA) on page 359
- After Installing Management Server High Availability (MX-HA) on page 362
- Monitoring Management Server High Availability (MX-HA) on page 365

Management Service-High Availability (MX-HA) Overview

The SecureSphere system comprises two main components, the gateway and the management server. Real time protection is the primary task of the gateway, whereas the management server's main roles are to configure the system, collect events from the gateway, analyze them and display resulting alerts.

The SecureSphere gateway is a mission-critical component — if a gateway fails, the Web and database servers behind the gateway are no longer protected. On the other hand, if a SecureSphere management server fails, protection is not interrupted.

A management server failure which continues for an extended period of time will impact the level of protection which the SecureSphere gateways provide, for the following reasons:

- **Profiling**: Application Profiling is performed by the management server based on data collected from the gateways.
- **Policies and Profiles**: No changes can be made to existing profiles or policies.
- **Alerts**: The gateway passes events to the management server, which stores and analyzes them and displays alerts derived from the events. If connectivity to the management server is down, the gateway saves events locally for later transmission, but the gateway will eventually overwrite older events as available disk space is reduced. When connectivity to the management server is restored and the gateway transmits its store of accumulated events to the management server, the management server will have incomplete data. Also, alerts normally pushed to predefined recipients via email now remain unnoticed.
- **Auditing**: This uses huge amounts of storage. These data are stored on the gateway, but unless archived regularly (a management server task) the newest auditing data are lost.



Note: In an MX-HA environent, there are many configuration changes which cannot be performed using the command line tools `impcfg` and `impctl`. For more information, see Command Line Tools and MX-HA on page 60.

Management Server-High Availability (MX-HA) Implementation

The Management Server-High Availability uses redundant management servers in a fully-automatic active/standby failover implementation, requiring no user interaction. The system senses the loss of the active server, and the failover mechanism begins. In the field the typical failover time period (which depends on the size of the system, and time elapsed since the last scheduled database synchronization) has been under measured as under 10 minutes, and the maximum time encountered was 30 minutes.

- The HA configuration comprises two management servers in the active/standby mode. Although only one server is active (i.e., managing the SecureSphere system), both servers are powered to allow database synchronization (using a standard Oracle process).
- Database synchronization is a scheduled process, the frequency and timing of which is decided by the system administrators. This means that whenever the active management server fails, there is **always** some data on its disk that is not mirrored on the standby management server.
- A heartbeat function (Linux) enables close monitoring of the active management server. During a server or network failure, the heartbeat function triggers the failover process and dispatches system logs to warn users that the active server requires attention.



Note: In the hosts files on each of the MX-HA servers, the host's name must appear **exactly** once.

Management Server High Availability (MX-HA) Components

The following components are included in the Management Server-High Availability solution:

- Linux Heartbeat on page 352
- Oracle Standby Database (Data Guard) on page 352
- SecureSphere Server on page 352
- HA Health Check on page 352
- Imperva Watchdog on page 352

Linux Heartbeat

Linux heartbeat is a Linux utility which enables implementing active-passive clusters. The heartbeat is the heart of MX-HA that is responsible for the database and management server and where they run.

The heartbeat configuration includes the following resources:

- Virtual IP address (VIP)
- database server.
- SecureSphere server

Once the heartbeat is started, all the resources are allocated to a specific server.

The heartbeat checks the status of the resources every minute. If one of the resources fails to run on the server, all resources are moved to the other server.

Oracle Standby Database (Data Guard)

Database synchronization is based on Oracle standby database (or Data Guard). Once MX-HA is installed, the database on the primary server is configured to support Oracle standby database. The database on the secondary server is deleted and copied from the primary server as a standby database.

After the installation, the standby database is constantly synchronized with the primary database using Oracle solution.

If the standby database fails to synchronize with the primary, it is recreated from the primary database.

SecureSphere Server

SecureSphere server is one of the resources in the heartbeat, but it is not modified during the MX-HA installation. The only change performed on the SecureSphere server is how it is started.

HA Health Check

In order to verify that everything is up and running, there is a health check mechanism that checks both servers. The heart of this mechanism is the **`healthCheck.sh`** script.

Imperva Watchdog

The Imperva watchdog script checks the heartbeat status, and if it is invalid, it restarts the heartbeat. The watchdog checks the heartbeat only after a successful start of the MX-HA using **`impctl`**. If MX-HA is stopped manually, it is removed from the watchdog's watch list.

Before Installing Management Server High Availability (MX-HA)

Hardware and Software Requirements

Management Server High Availability (MX-HA) requires a specific hardware and software configuration:

- Two management servers

  Management Server High Availability cannot be installed on gateways or one box solutions.
- You must have licenses for both servers.
- Both servers must have the same amount of memory (RAM).
- It is recommended that both servers have the same amount of disk space, otherwise failover to a server with less disk space will negatively impact performance and can in some circumstances even fail (for example, when the server needs more space than the failover machine can allocate).
- Both servers must have the same version of SecureSphere release installed.

  Management Server High Availability is supported in SecureSphere versions 6.0.5.6238 and later.
- Each server must have the following two network interfaces:
  - An interface for public network.
  - An interface for interconnect (using cross-link cable or other connection) to the other server. This interface is used by Linux heartbeat and by Oracle to synchronize the standby database.
- SSH trust between the servers for both `root` and `oracle` users.
- Well-defined and unique host names on both servers.

Pre-Installation Tasks



Note: The public IP addresses of both MX servers must be on the same subnet. If the servers are located at different sites, there must be a VLAN between the sites with the same subnet.

Install the Latest Patch

1. Install the latest patch to your version of SecureSphere on **both** management servers.
2. Reboot both management servers.

For information about downloading and installing patches, see the Imperva support site.

Configure the Interconnected Interfaces

The interconnected network must be defined during the first-time login procedure on the management server by setting up the LAN interfaces. If this was not done during the first-time login, the LAN interfaces can be configured now using `impcfg`.

To configure the interconnected interfaces on the management server:



Note: Both interconnected interfaces must be on the same subnet.

3. Perform the following on both management servers:
   3.1 Start **impcfg**.
   3.2 In the **Top** Screen, select **3) Manage platform**.
   3.3 In the **Platform Management** Screen, select **1) Manage network**.
   3.4 In the **Network Management** Screen, select **2) LAN interface**.
   3.5 Configure all three options:
   3.6 Change device
   3.7 Change IP address
   3.8 Change IP netmask
   3.9 Return to the **Top** screen by selecting option **t**.
   3.10 Apply the settings by selecting option **A**.

Test the Interconnected Interfaces

To test the interconnected interfaces:

4. Ping from the first management server to the second management server on its internal interface.
   The ping will fail, because the management server blocks ICMP by default.
5. Immediately after the ping, execute **arp -a** and locate the arp entry of the other server.
   If the arp entry has a valid MAC address for the other server, the interconnect was successfully configured.

Download the RPMs and Prepare the Servers

On both servers, perform the following:

6. Login as user **root**.
7. Execute the following command:

```
mkdir /var/tmp/mxha
cd /var/tmp/mxha
```

8. Navigate to the appropriate **MX-HA** directory on the Imperva FTP site (**ftp-us.imperva.com**).
   The directory names are listed in the table below.

HA RPM Directories

	Directory Name
32 bit	/Downloads/SecureSphere_Setup/v9.5/32Bit/MX-HA/
64 bit	/Downloads/SecureSphere_Setup/v9.5/64Bit/MX-HA/

9. Download both of the files in the **MX-HA** directory to the **/var/tmp/mxha** directory.

The names of the files to download are listed in the table below.

HA RPM Files

	File Names
32 bit	`oracle-EE-11.1.0.7.3-1.i386.rpm` `oracle-EE-bin-11.1.0.7.3-1.i386.rpm`
64 bit	`oracle-EE-11.1.0.7.3-1.x86_64.rpm` `oracle-EE-bin-11.1.0.7.3-1.x86_64.rpm`

10. Execute the following command:

```
impctl server ha preparerpm
```

Set Up Hostnames

To define hostnames:

11. On both management servers, edit the `/etc/hosts` file and add the hostnames and public IP addresses of both management servers.

```
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1       localhost.localdomain localhost localhost1
10.1.12.111     node1
10.1.12.134     node2
```

Figure 72 /etc/hosts File

12. Verify that there are no duplicate names in the file.



Note:
- There is no need to add the private or the virtual IP address.
- In the `hosts` files on each of the MX-HA machines, the host's name must appear **exactly** once.
- The hostname may not include the "-" character.

13. On both management servers, execute the following commands:

```
impctl hardening config --root-source-ip-exception=<vip>
impctl hardening config --root-source-ip-exception=<other_MX private interconnect>
impctl hardening config --root-source-ip-exception=<other_MX physical>
```

where:

- `<vip>` is the floating IP address, that is, the IP address shared by both management servers.
- `<other_MX private interconnect>` is the IP address of the interconnect on the other management server; for example when you are running this command on the primary management server, specify the IP address of the interconnect on the secondary management server.
- `<other_MX physical>` is the public IP address of the other management server; for example, when you are running this command on the primary management server, specify the public IP address of the secondary management server.

Configure SSH Trust for User Root

To configure SSH trust for user root:

14. Connect to a management server using SSH as user **root**.



Note: To connect as user root over SSH, you must connect as a CLI user other than **root** and **secure** and use the **admin** command. For more information, see CLI Users on page 57.

15. Execute the following command:

    ssh-keygen -t dsa

16. In response to each of the prompts, press Enter.

```
[root@node1 ~]# ssh-keygen -t dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/root/.ssh/id_dsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_dsa.
Your public key has been saved in /root/.ssh/id_dsa.pub.
The key fingerprint is:
b7:1a:19:c9:73:70:7a:6e:b0:f5:38:31:de:fc:71:af root@node1
[root@node1 ~]#
```

17. Execute the following command:

    cp ~/.ssh/id_dsa.pub ~/.ssh/authorized_keys

18. Perform steps 14. through 17. on the second management server.

19. Edit the **~/.ssh/authorized_keys** file on both management servers, so that the files on both management servers contain the keys of both management servers, as follows:



Warning: Read all these instructions before executing the first one, and then execute each step carefully and exactly as written.

19.1 On the first management server, execute the following command:

cat ~/.ssh/id_dsa.pub

```
[root@node2 ~]# cat ~/.ssh/id_dsa.pub
ssh-dss AAAAB3NzaC1kc3MAAACBAJ/5FzCECR5v51yC1S7ExiMx1VnkO6oQEG9fdTkcQzZKHgsPSZtB
OI+31qRWP4zjVfS5DwXcKpkihNTUVCjForOOKOEJ+JKk4yLe3uqqLUEVIHwmSTwKz3N6bfvBC3olzFc7
BDOTbyJzg51S+reqsrCt3wny2JNTpsqBUaUBF9fjAAAAFQDf7QwL3OjDyOdMo/iDZreAwmuAaQAAAIA3
WAaON3SmGykBqzLIhPbPjXcQFGTqi5NDV4O6kO9NZ4vUga3BuC6X5TmpbVRyiFVwxO1ifU8K+UumDyKB
2rkJ7dKGuBCekme1dE4wlySyGax1JhNXOz4ihhoOZF9zf+GMTFwALphZPKo192Ov67n/aqNQAfcwMGOj
5/ouvvlAGQAAAIARGqhm4j3t6reLgCVUag/oiV11VwpjOvj4kBIVZqUc7QacFkJRqVjCuTotdAuP+R7F
LhQwJloxZe36NZaT94RgFXOFpzro5dozHKt3ac/1rW33IucyKATVed1tPvbRqZUsUX4B1F8e2zxevNho
jLtOTcE4Sj1OWql4DAYOKOP4Vw== root@node2
```

19.2 Copy the output to the clipboard.

Make sure you select only the output, without the trailing new line.

19.3 In the other management server terminal session, enter the **echo** command but *do not press Enter.*

19.4 Paste to the data that was copied earlier to the clipboard into the other management server terminal session.

19.5 Add the following text at the end of the command you are putting together:

>> ~/.ssh/authorized_keys

You have now constructed a command from three elements (see the screen shot below):

- the word “echo”
- the clipboard data
- the >> redirection



19.6 Press Enter.

20. On both management servers, check the SSH connection using the following command:

    ssh <other-server-hostname> date

    The command should run without asking for a password.

Configure SSH Trust for User Oracle

To configure SSH trust for user oracle:

21. Connect to a management server using SSH as user **root**.



Note: To connect as user root over SSH, you must connect as a CLI user other than **root** and **secure** and use the **admin** command. For more information, see CLI Users on page 57.

22. Execute the following command:

    su - oracle

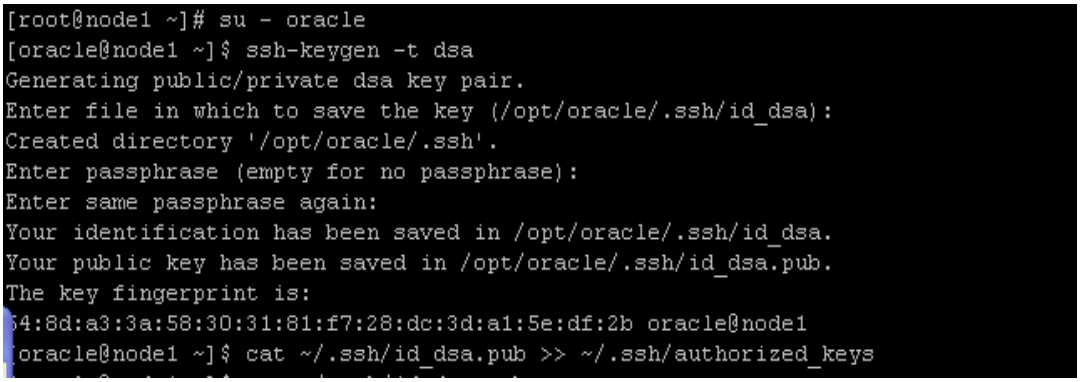
23. Execute the following command:

    ssh-keygen -t dsa

24. In response to each of the prompts, press Enter.

25. Execute the following command:

    cp ~/.ssh/id_dsa.pub ~/.ssh/authorized_keys



26. Perform steps 21. through 25. on the second management server.

27. Edit the **~/.ssh/authorized_keys** file on both management servers, so that the files on both management servers contain the keys of both management servers, as follows:

Warning: Read all these instructions before executing the first one, and then execute each step carefully and exactly as written.

27.1 On the first management server, execute the following command:

```
cat ~/.ssh/id_dsa.pub
```



27.2 Copy the output to the clipboard.

Make sure you select only the output, without the trailing new line.

27.3 In the other management server terminal session, enter the **echo** command but *do not press Enter.*

27.4 Paste to the data that was copied earlier to the clipboard into the other management server terminal session.

27.5 Add the following text at the end of the command you are putting together:

```
>> ~/.ssh/authorized_keys
```

You have now constructed a command from three elements (see the screen shot below):

- the word “echo”
- the clipboard data
- the >> redirection



Figure 73 The constructed command

27.6 Press Enter.

28. On both management servers, check the SSH connection using the following command:

```
ssh <other-server-hostname> date
```

The command should run without asking for a password.

Installing Management Server High Availability (MX-HA)

MX-HA is installed on an already functioning MX. You should have two management servers, one of which you designate as primary and the other as secondary.

To install MX-HA:

1. Perform the pre-installation tasks (see Pre-Installation Tasks on page 353).
2. Upload licenses for both the primary management server and the secondary management server to the primary management server.

   Alternatively, you can upload only the primary management server license, install MX-HA on the primary server and install the secondary license (on the primary management server) at a later time. This alternative is not recommended, because it temporarily leaves the configuration without a license for the secondary management server, but it can be done.
3. Login to the primary management server as user `root`.



Note: The installation is performed only on the primary server. The secondary server is installed as part of the installation of the primary server, and any data on the secondary server is deleted.

4. On the primary server, execute the following command, entering parameters as listed in Table .

```
impctl server ha install
```

Installation Parameters

Parameter	Description	Default Value
Installation Directory	The directory in which MX-HA will be installed.	`/opt/secsph-ha`
Directory for temporary data	The directory in which temporary files will be written during the installation process.	`/var/tmp/secsph-ha`
Keep alive IP address (pingable server)	This IP address is used to check the network status. You can use any IP address on your network as long as it remains constant, active and pingable. If the keep alive address does not respond to the ping, a fail over occurs.	
Secondary server public IP address	The public address of the secondary management server.	
Virtual server IP address	The IP address used to access the MX-HA servers.	
Heartbeat interface name	The interface which is the direct connection between the two management servers.	
Public interface name	The management interface name.	

Installation Parameters

Parameter	Description	Default Value
sys user password	The password for the sys user in the database. This password must be entered a second time for verification. **Note:** The password can contain any combination of lowercase letters, uppercase letters, numbers and the following special characters: !#%^*()	

The screen shots below show a typical installation.

Note: You have the option of exporting the database before the installation. You can export the database before installing MX-HA, or optionally, during the MX-HA installation (see Figure 74).

```
Enter the keep alive IP address (pingable server): 10.1.1.254
Enter the secondary server public IP address: 10.1.12.36
Enter the virtual server IP address: 10.1.12.35
Enter the heartbeat interface name: eth1
Enter the public interface name: eth0
Enter new password for sys user in the database:
Enter new password for sys for verification:

Starting HA installation on: Tue Dec  1 16:08:04 IST 2009
Log file for installation is /var/log/ha-install.log
Configuration:
   Installation directory: /opt/secsph-ha
   Directory for temporary data: /var/tmp/secsph-ha
   keep alive IP address: 10.1.1.254
   Secondary server public IP address: 10.1.12.36
   Virtual server IP address: 10.1.12.35
   Heartbeat interface name: eth1
   Public interface name: eth0
Are these parameters OK? [y/n]
y
Do you wish to perform full export before the installation? [y/n]
```

Figure 74 MX-HA Installation - part 1

```
local IP: 10.1.4.71

Configuring portguard and icmp... Done

Checking pre-requirements... Done

Primary server is:     node1
Secondary server is:   node2

Updating clocks... Done

Creating necessary directories... Done

Modifying user oracle... Done

Removing management server and database services from impctl... Done

Installing and configuring HA services... Done

Installing support scripts... Done

Exporting license configuration:
   Primary server... Done
   Secondary server... Done

Configuring impctl parameters for HA... Done

Changing sys password... Done

Creating Oracle HA configuration:
   Configuring Oracle network... Done
   Configuring primary database... Done
   Configuring standby database... Done

Stopping non-HA services... Done

Updating oracle crontab and logrotate... Done

Restarting HA services:
   Stopping HA services... Done
   Starting HA services (this may take up to 20 minutes)...


Done

HA installation completed successfully at Sun Apr 27 13:52:20 IDT 2008
[root@node1 tmp]#
```

Figure 75 MX-HA Installation - part 2

After Installing Management Server High Availability (MX-HA)

Verify the Primary Server is Active

Once the installation is completed, verify that the primary server is active and running.

To verify that the primary server is active and running:

1. Execute the following command on both the primary and secondary servers:

```
impctl server ha status
```

The following output should appear:

```
started,ip-on-node1,db-on-node1,server-on-node1,running
```

status Command Output Explanation

	Explanation
`started`	heartbeat status
`ip-on-node`	the host that owns the active Virtual IP address (VIP)
`db-on-node1`	the host that owns the active database
`server-on-node1`	the host that owns the active management server
`running`	status of the active host

Register the Gateway

After installing MX-HA, the gateway must be (re)registered with MX-HA.

To register the gateway:

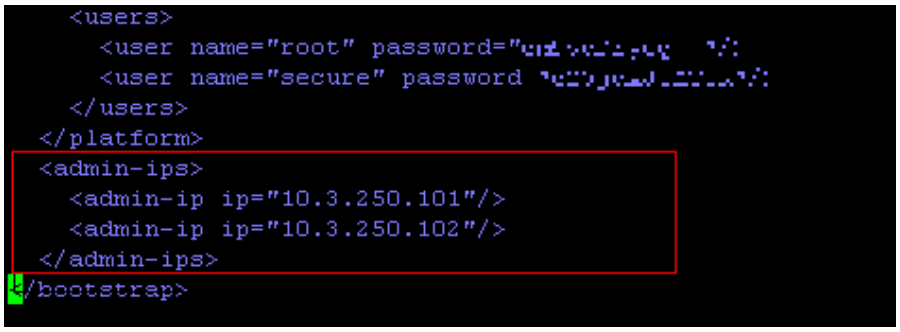
1. Configure `admin-ips` in the `bootstrap.xml` file.
2. Re-register the gateway using the virtual IP address (VIP) of the management servers.

admin-ips

1. Add the following xml part to the `bootstrap.xml` file on each of the gateways (`/opt/SecureSphere/etc/bootstrap.xml`):

```
<admin-ips>
 <admin-ip ip="server-real-ip1"/>
 <admin-ip ip="server-real-ip2"/>
</admin-ips>
```

Substitute the servers' real IP addresses (inside double quotes) for **server-real-ip1** and **server-real-ip2**s.



Re-registration

After the installation process has successfully finished, re-register the gateway using the MX-HA virtual IP address.

Uninstalling MX-HA

To uninstall MX-HA solution, the primary server must be available, otherwise, there is no guarantee that the uninstall process will successfully complete.

To uninstall MX-HA:

1. Login to the primary MX server as user **root**.
2. Execute the following command:

```
impctl server ha uninstall
```

```
[root@node1 ~]# impctl server ha uninstall

Starting HA uninstall on: Mon Apr 28 13:45:38 IDT 2008
Log file is /var/log/ha-uninstall.log

Are you sure you want to uninstall MX high availability? [y/n]
y

Checking Database status... Done

Other server (10.1.4.73) is available - uninstall will be performed on both servers
Database on other server (10.1.4.73) will be deleted

Deleting oracle crontab and logrotate changes... Done

Removing Oracle HA configuration... Done

Stopping HA services... Done

Changing sys password... Done

Starting database on primary... Done

Removing Oracle network configuration... Done

Removing HA database configuration... Done

Stopping database on primary... Done

Enabling non-HA services to impctl and removing HA service... Done

Removing HA configuration and scripts... Done

Removing portguard and icmp configuration... Done

Starting services... Done

Deleting database from secondary server (10.1.4.73)... Done

HA uninstall completed successfully at Mon Apr 28 13:56:27 IDT 2008
```

Once the uninstall process is complete, the primary server functions normally as a single server. The secondary server is unusable, and its database must be recreated using the following command:

```
impctl db create
```

Changing Database and/or System Passwords

To change the system (database) and/or secure (system) password on the primary management server, use the following command:

```
impctl server ha password
--set-database-password=NEW_SYSTEM_PASS
--set-server-password=NEW_SECURE_PASS
```

Monitoring Management Server High Availability (MX-HA)

This section includes the following:

MX-HA Status on page 365
Confirming that MX-HA is Correctly Configured on page 365
MX-HA Logs on page 367
Heartbeat Behavior on page 368
Known Issues on page 369
File List on page 370

MX-HA Status

1. The **impctl** command displays the status of MX-HA. The command syntax is as follows:

```
impctl server ha status
```

This command returns if the MX-HA is started, and on which server the resources are running. The output of this command returns the server that holds each resource (IP, database and server) even if only some resources are up.

When all the resources are running, the MX-HA is running and the SecureSphere server is available.



Note: When you run this command on a secondary MX, it shows the status of the primary MX.

Confirming that MX-HA is Correctly Configured

After configuring MX-HA, you may wish to confirm that the configuration is correct rather than to wait for the primary MX to fail. This section describes the following:

Initiating a Failover in an MX-HA Environment on page 365
Confirming That the MX-HA Servers are Synchronized on page 366

Initiating a Failover in an MX-HA Environment

This section describes how to perform a safe and successful failover in MX-HA. A failover is sometimes required for testing.

To initiate a failover:

1. Execute the following command on both MXs:

```
impctl server ha status
```

If HA is running on both MXs, the output on each MX should resemble the following:

```
started,ip-on-r2d2,db-on-r2d2,server-on-r2d2,running
```

2. Confirm that the MXs are synchronized (see Confirming That the MX-HA Servers are Synchronized on page 366).
3. Initiate a failover as follows:
   3.1 Stop the primary MX by executing the following command:

```
impctl server ha stop
```

   3.1 Wait until the secondary MX becomes active (that is, it has become the primary MX). You can determine whether it is active by using the following command:

```
impctl server ha status
```

   If the secondary MX is now the primary MX, that is, if failover has successfully occurred, the output should resemble the following:

```
started,ip-on-r2d2,db-on-r2d2,server-on-r2d2,running
```

   At this point, the MXs have switched roles:
   - The MX that was formerly the secondary MX is now the primary MX, and its GUI is now usable.
   - The MX that was formerly the primary MX is now the secondary MX, and is down (you stopped it in step 3.1).

5. Start the secondary MX (the MX you stopped in step 3.1) by executing the following command:

```
impctl server ha start
```

   The secondary MX now has to perform a full synchronization with the primary MX, and it is not yet ready for failover.
4. To determine when the standby MX has re-synchronized and is ready for failover, follow the instructions in Confirming That the MX-HA Servers are Synchronized below.

Confirming That the MX-HA Servers are Synchronized

This procedure describes how to verify the status of an MX HA server.

To verify the status of an MX-HA server:

1. Login as root to the secondary MX.
2. Check the last entries in **`healthChek.log`** file (usually located in **`/opt/secsph-ha/`**) and confirm that:
   - the date and time of the entries are recent
   - the status is "**`Database is standby`**"
   - lag is `0`

For example,

```
[01/30/12 11:05:03 healthCheck] - healthCheck started
[01/30/12 11:05:03 healthCheck] - Server role: secondary server
[01/30/12 11:05:06 healthCheck] - Attempt 1 out of 5
[01/30/12 11:05:06 healthCheck] - Database should be standby
[01/30/12 11:05:06 healthCheck] - Database is standby
[01/30/12 11:05:06 healthCheck] - Checking standby synchronization...
[01/30/12 11:05:10 healthCheck] - Lag is: 0 (primary seq: 3785)
```

MX-HA Logs

healthCheck.log

The **healthCheck.log** file is located in the MX-HA installation directory. It is a general log, which contains information about the heartbeat status, the role of the server, and the status of the database.

The structure of the log is as follows: [<date> <time> <component>] - <message>.

The following are the main components that write to the log:

- **Ha-dbora** is responsible for managing the database. **Ha-dbora** writes to the log when the heartbeat is requesting to stop, start or get status of the database server. This component runs only on the primary server.
- **Ha-secsph** is responsible for managing the SecureSphere server. **Ha-secsph** writes to the log when heartbeat is requesting to stop, start or get status of the SecureSphere management server. This component runs only on the primary server.
- **healthCheck** is responsible for the database health on both servers. This component checks if the server is the primary or secondary, and according to the answer verifies that the database is in the correct status. If needed, this component runs other components to recreate and standby database or changing the standby database to primary.
- **syncDirs** is responsible for synchronization of directories and files from the primary server to the secondary server, this is done using **rsync** utility and according the **rsync.conf** file. This component runs only on the secondary server.
- **watchdog**: every time the watchdog checks the heartbeat status, it writes information to the log file about the current status and whether it is going to restart the heartbeat or not.
- When there is a failover, or the standby database is not valid, all the information about the failover or the creation of the standby database is written to this log.

/var/log/ha-log

- The **/var/log/ha-log** file is the log of the Linux heartbeat. This log contains information about the cluster, resources and transition between the servers.

  Certain information from MX-HA is written to this file as well as to the **healthCheck.log**. This information is mainly from **ha-dbora**, **ha-secsph** and the **watchdog**.

alert_secsph.log

This file is the Oracle database log, and contains information from Oracle database, including information relevant to the standby solution. The log is located under the **/opt/oracle/admin/secsph/bdump** directory, assuming that **/opt/oracle** is the Oracle installation directory.

Heartbeat Statuses

MX-HA uses the Linux heartbeat solution. Part of the heartbeat is the Cluster Resource Manager (CRM), which takes care for the group of resources and handles starting, stopping and moving them between the servers.

MX-HA uses **/usr/lib/heartbeat/crmadmin** to determine where the resources are running and the status of each server.

Resource Status

To determine where a resource is running, MX-HA uses **crmadmin -W <resource>,** where **<resource>** is one of the following:

- **PrimaryGroup:ip_resource**, **PrimaryGroup:OracleDB**
- **PrimaryGroup:SecureSphere**

The output of this command is the server name that holds the resource, or a message if the resource is not running or nothing if the heartbeat is down.

The **impctl server ha status** command uses the **crmadmin** to list the owners of the resources.

The **healthCheck** script uses **crmadmin** in order to decide which server is the primary, that is, the server that holds the IP resource.

Server Status

To determine the server status, MX-HA uses the **crmadmin -S <hostname>** command. The output of this command is the current status of the server.

The two most important statuses are **S_IDLE** and **S_NOT_DC**. Both statuses mean that the server is idle, either primary or secondary. Other statuses, such as **S_ELECTION**, **S_TRANSITION_ENGINE**, **S_STARTING** and so on, meaning that the server is performing a task, such as starting, stopping, change status from primary to secondary and so on.

impctl watchdog

The **watchdog** is responsible for health checking of the management components. In a regular management configuration, the **watchdog** verifies that the database and the SecureSphere server are working properly.

Under MX-HA configuration, the **watchdog** command does not check the database or the server. It checks only the heartbeat.

Every time the **watchdog** runs, it checks the heartbeat status and the owner of the IP resource. If the status is not idle or if **crmadmin** returned nothing, it means that everything is functioning properly.

The **watchdog** restarts the heartbeat, if the heartbeat is idle and but the IP address is not running on both nodes.

Heartbeat Behavior

Failover Sequence

The heartbeat uses the internal scripts **ha-dbora** and **ha-secsph** to verify the status of the IP address, database and SecureSphere server. If one of the resources has an invalid status, the heartbeat stops higher resources. If IP address is down, both database and SecureSphere server are stopped. If the database is down, only the SecureSphere server is stopped.

Then, the heartbeat tries to start the failed resource again. If the start is successful, heartbeat continues to start all other dependent resources. If the start operation fails, heartbeat performs failover and moves all the resources to the other server.

During a failover, the heartbeat stops all the resources on the primary server (server A) and starts them on the other server (server B). At this time, server A is in the TRANSITION status. When server B finishes starting all the resources, server A status becomes **S_IDLE**, and since the database on server A is not standby, it is recreated.

When the process completes, server A is still in the **S_IDLE** status, which is invalid for the secondary server. At this time, the watchdog restarts the heartbeat on server A and the entire environment is valid again.

If during the failover from server A to server B, one of the resources could not start on server B, the heartbeat stops everything on both servers. At this point, the **watchdog** command restarts the heartbeat on both servers.

In addition, failover occurs when the primary server reboots or the **server-ha** service is stopped.

Standby Recreation

The standby database is constantly being synchronized with the primary database. There are several situations in which the standby database is recreated. This means that the database is deleted, and is copied from the primary database, as follows:

- The standby database has a lag higher than a certain level. The level is configured in the **bootstrap.xml** file, and its value is 10 redo logs by default.
- The healthcheck process cannot check the synchronization level.
- The database is not a valid standby. For example, after a failover, the new secondary server contains a primary database and not a standby database. In this case, the database on the new secondary server is recreated.

The standby database can be recreated only if the primary database and server are running. Otherwise, the standby writes a message to the **healthCheck.log** and is not recreated.

Known Issues

MX-HA Installation Failure

A failure of the MX-HA installation procedure does not invoke an uninstall process. Before proceeding, you must “clean up” the unsuccessful installation on the primary server and re-initialize the database on the secondary server.

1. On the primary server, execute the following command:

```
impctl server ha uninstall
```

2. On the secondary server, execute the following command:

```
impctl db start
```

Failure While Building the Standby Database

In very rare cases, the standby database needs to be recreated. The creation process can take some time, and during this time the standby database is not operational and cannot become the primary database. If there is an unrecoverable failure on the primary server while the standby is recreated, MX-HA cannot overcome this failure. In some cases, a manual intervention can solve the problem, but in other cases there is no solution.

For example, if the database files are deleted from the primary server during the standby recreation, there is no valid database to use, and MX-HA or manual operations cannot start the system.

If this occurs, contact Imperva support.

Management Server Replacement

Currently, there is no supported option to install only a secondary server in the MX-HA solution. If the secondary server crashes and needs to be replaced, replace it using the following procedure:

1. Uninstall MX-HA from the primary server.
2. Connect and configure the new secondary server, including all prerequisites.
3. Reinstall MX-HA from the primary server.

File List

The following files are installed when the MX-HA is installed:

MX-HA File List

File Name	Description
`cib.xml`	This file is the heartbeat configuration file. This file contains the heartbeat resource configuration including the operations, timeouts and scripts.
`ha-dbora`	This file is located under `/etc/init.d` and handles the operations that heartbeat can do on the database, including start, stop and status. Currently, this script also checks ping to the gateway to verify that the network is available.
`ha-secsph`	This script is located under `/etc/init.d` and handles the operations that heartbeat can perform, including start, stop and status.
`creConfig.sh`	This script creates data guard configuration after creating a standby database.
`deconfigNet.sh`	This script removes the Oracle net configuration, and is used when uninstalling MX-HA.
`deconfigPrimary.sh`	This script changes the primary database back to stand-alone database, and is used when uninstalling MX-HA.
`failover.sh`	This script performs data guard failover to change a standby database to the primary database.
`getInfo.sh`	This script is used to get information about the database. The information is the database role (primary or standby) and database status (down, started, mounted or open).
`getSeq.sh`	This script is used to get the current redo log sequence of the local or remote database.
`healthCheck.sh`	This is the main script.
`healthcheckmasterDB.sh`	This script checks the status of the database and performs ping to the gateway in order to verify that the network and database are healthy. If something is not valid, the script returns an error and the heartbeat identifies that the resource is down.
`healthcheckmasterJAVA.sh`	This script is similar to `healthcheckmasterDB.sh`, but checks SecureSphere server.
`instPrimary.sh`	This script changes a stand-alone database to the primary database in an MX-HA configuration. This script is executed during the MX-HA installation process.
`instStandby.sh`	This script recreates the standby database from the primary database.

MX-HA File List (continued)

File Name	Description
`modnet.sh`	This script is for setting up the Oracle network. This script is executed only once, during the MX-HA installation process.
`resync_standby.sh`	This script is used when the standby is not valid. This script deletes the data guard configuration, recreates the standby database and creates the data guard configuration using the relevant scripts.
`rmArch.sh`	This script handles deletion of archived redo logs from both primary and secondary servers. This script is executed by the **`crontab`**.
`rmDGConfig.sh`	This script removes the Oracle Data Guard configuration, and is used before recreating the standby database.
`rsync.conf`	This file contains all the files and directories that need to be synchronized from the primary server to the secondary server.
`shutDB.sh`	This script is used to shutdown the database.
`standby.conf`	This file is a general configuration file that contains extraction of information from the **`bootstrap.xml`** file and general functions that are used by other scripts.
`startDB.sh`	This script is used to start the database.
`syncDirs.sh`	This script synchronizes files and directories from the primary server to the secondary server according to the **`rsync.conf`** file. This script is executed by **`ha-dbora`** every time heartbeat requests database status.

CHAPTER 18

Network High Availability

In addition to high availability provided by both the management server and the Gateway, the network itself can also be used to reach high availability This option relies on a mechanism which detects when an opposing network interface is down, and subsequently takes the operating interface on the opposite side of the network link offline to prevent data from being sent to an inoperative interface.

Once the problematic network interface becomes available, the SecureSphere appliance gives the operating interface (which was manually taken down) a period of time to come up and stabilize. If it does not succeed, then the original interface is taken back offline. This is in order to prevent a situation in which the interfaces get involved in an ongoing pattern of going up and down. The amount of time given for the interface to come back up is configurable by editing a supporting file.



Note: This chapter describes how to achieve high availability through the network. It detects link status and enables HA only if it is network related. It does not facilitate HA when an issue is software related. For information on how to provide HA in these cases, see Management Server High Availability (MX-HA) on page 349 or Gateway High Availability on page 339.

This chapter includes the following:

Network High Availability Support on page 373

Configuring Network High Availability on page 373

Network High Availability Support

Network high availability is supported in bridge mode (STP / Impvha). It is not available in Kernel Reverse Proxy or sniffing modes. The following table lists the interface types and their support for network high availability.

Interface Support for Network High Availability

Interface Type	G-Series	X-Series
Copper	Supported	Supported
1 G	Not Supported	Supported
10 G	Not Supported	Not Supported
10 G with Bypass Support	Not Supported	Supported

Configuring Network High Availability

You can configure the amount of retries, and subsequently the period of time that is provided for the operating interface to come back up.



Note: This procedure should only be conducted after consulting with a member from the Imperva support team.

To modify the number of retries for an interface:

1. Navigate to the following location on the SecureSphere appliance:
   opt/SecureSphere/etc
2. Access the following file:
   hades.cfg
3. Modify the following parameter:
   bridge_relief_count_[#]
   where [#] is the value for the number retries you want SecureSphere to attempt before it manually takes the interface offline.

Default: 5 retries (10 seconds)

Please note that each retry is made after 2 seconds. So the overall amount of time an interface is given to come back up is the number of retries multiplied by 2.

EXAMPLE:

If you set the parameter to: **bridge_relief_value_1**

It attempts 1 retry after two seconds, or give the interface 2 seconds to come online until the original interface is taken down again.

If you set the parameter to: **bridge_relief_value_6**

It attempts 6 retries two seconds apart, or give the interface 12 seconds to come online the original interface is taken down again.

APPENDIX A

Installing SecureSphere From the Network

This chapter describes how to install and configure SecureSphere remotely, and includes the following:

- Installing from the Network on page 375

Installing from the Network

Introduction

Network deployment is a process in which a Deployment Server installs a new SecureSphere build on a target appliance through a direct cable connection. Installation can also be performed using regular cables through a hub or switch, or even using existing network connectivity, as long as there is no active DHCP Server on the network.

The installation is done using PXE (pre-boot execution environment). PXE is an environment to boot computers using a network interface independently of available data storage devices (like hard disks) or installed operating systems.This environment can be invoked from the console of a target appliance when it is booted.

SecureSphere network installation consists of two steps:

1. Preparing the Deployment Server

   A Deployment Server is a Windows machine, typically, a laptop, or any machine that can be physically connected to the target appliance. The SecureSphere Network Deployment Package must be obtained from the Imperva FTP site and installed on the Deployment Server.



Note: This step needs to be performed only once for each new SecureSphere release.

2. Attaching either a VGA or serial console to the target appliance.



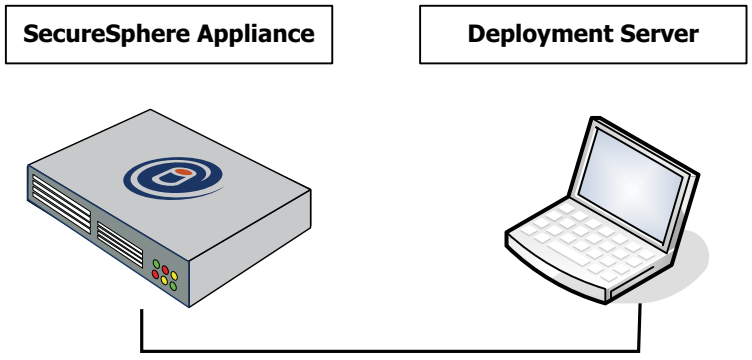
Note: VGA consoles can only be connected to G-series appliances. X-series and M-series appliances do not have a VGA port.

   The progress of the installation is displayed on the console.

3. Running the Network Installation

   Once the two machines are connected, start the Network Deployment application on the Deployment Server.

   The target appliance is booted and installs itself through the network using the connection between the machines.



Cable connecting the Deployment Server's LAN Interface and the Target Appliance's Management Interface

Figure 76 Connecting the Deployment Server to the Target Appliance

Preparing the Deployment Server

Obtaining the Network Deployment Package

Download the installation package from the Imperva FTP site. The file names are listed in the table below.

	Location
32 bit	`/Downloads/SecureSphere_Setup/v9.5/32Bit/Network/`
64 bit	`/Downloads/SecureSphere_Setup/v9.5/64Bit/Network/`

Login information to the support FTP site should be obtained along with license information. If you do not have credentials, please contact Imperva support.

Installing the Package on the Deployment Server

Once the Network Deployment Package is obtained, install it on the Deployment Server. The installation requires ~1.5 GB of free space. By default, it will try to install the package in the directory `C:\Program Files\Imperva\SecureSphere <version> Network Deployment Tool`

If you do not have sufficient available disk space on `C:\` change the directory during the installation.



Note: If the server IP and connectivity were not yet set, un-check option “Start the Imperva.inc Network deployment tool now”.

Configuring the Deployment Server IP Address

You need to adjust the network address of the Deployment Server, so that it can communicate with the target appliance. To achieve that, you need to modify the TCP/IP settings of the interface, to be static, preconfigured IP.

To modify the TCP/IP settings:

1. From the Start Menu, select **Settings** > **Network Connections**, select the relevant LAN connection (typically on a laptop it is Local Area Connection), right click on it, and select **Properties**.
2. In the **Properties** dialog box, select **Internet Protocol (TCP/IP)**, and click **Properties**.

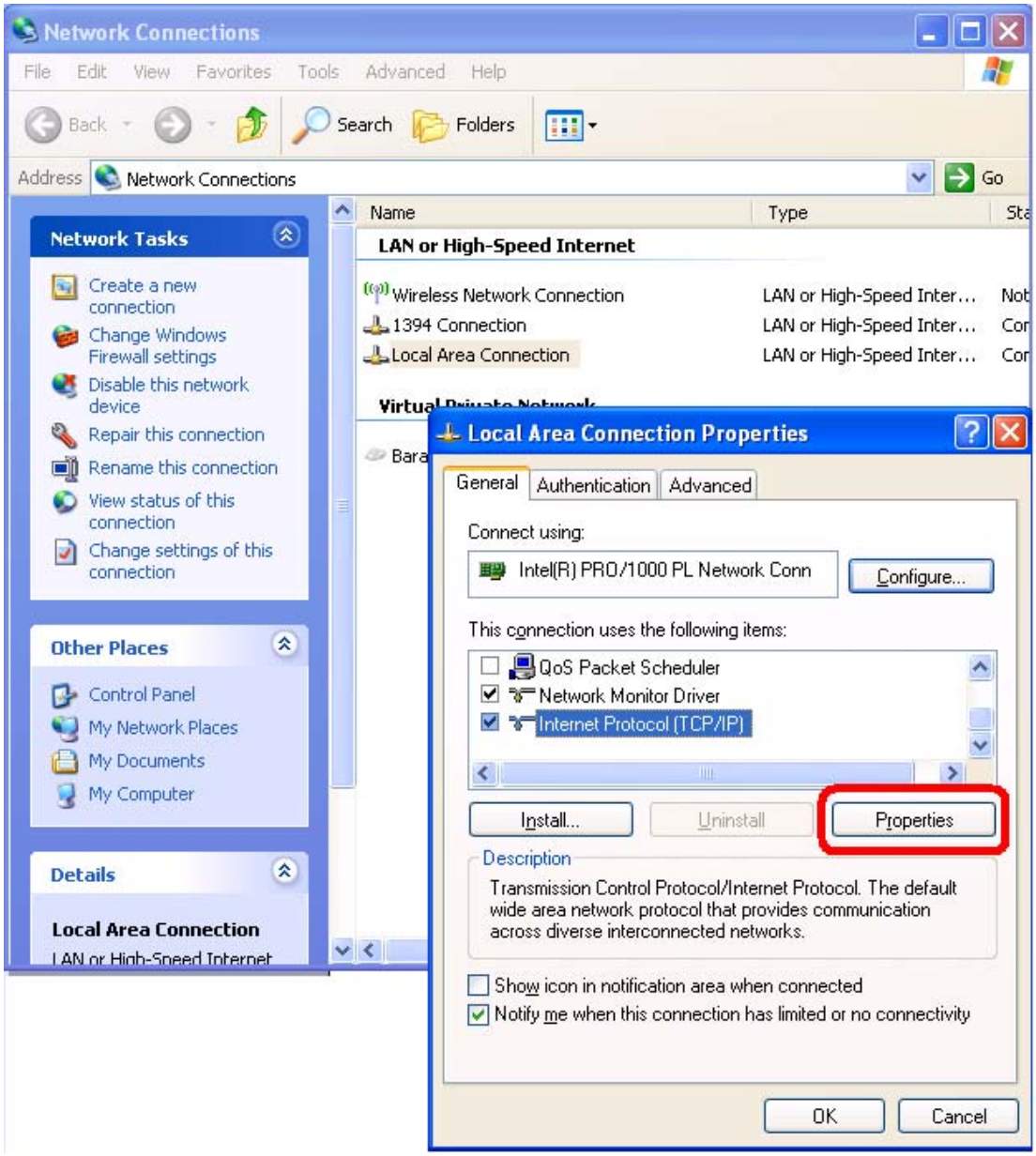


Figure 77 Changing TCP/IP Settings

3. Fill in the fields as displayed, with the IP 10.0.0.1, mask 255.0.0.0 and click **OK**.

Warning: You must enter the 10.0.0.1, as currently this is the only supported IP address.

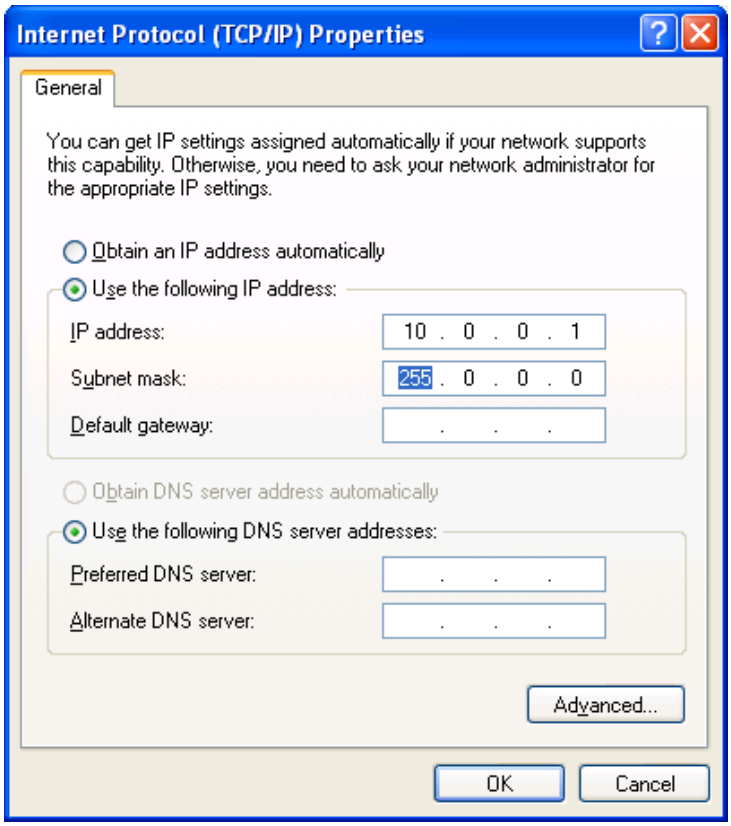


Figure 78 TCP/IP Properties window

4. Now the Deployment Server is ready to accept deployment requests from the appliance.

Running a Network Deployment

Connecting the Target Appliance and Deployment Server

To connect the target appliance to the deployment server:

1. Make sure that your installer machine and target appliance are close enough to be physically connected, or that they have a shared connection switch.

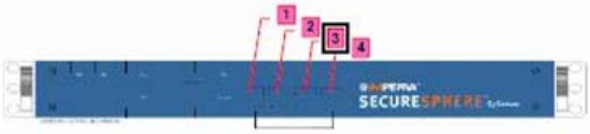


Figure 79 Interface Setting for G2 appliance

2. For a G2 appliance, connect the deployment server and the target appliance using a **cross cable** and the fail-close interface (**number 3** in the figure above).
3. For other appliances than G2, connect the cable to the appliance's Management Interface (as defined in the Quick Start Guide of the appliance, usually one of the two on board interfaces). When the appliance tries to boot from the network, it will try both of the on board interfaces, one after the other.

Running the Deployment Program on the Deployment Server

The deployment program (installed as part of phase 1) contains the following components:

- DHCP Server
- TFTP Server
- FTP Server

To launch the deployment program:

1. From the Start Menu, select **Programs** > **Imperva** > **SecureSphere <version> Network Deployment Tool**. The dialog below, allows you to monitor the installation processes.
2. The software will fail to load if the interface is not linked and/or the IP address is not set according to the instructions. See Configuring the Deployment Server IP Address on page 376 for configuration details.

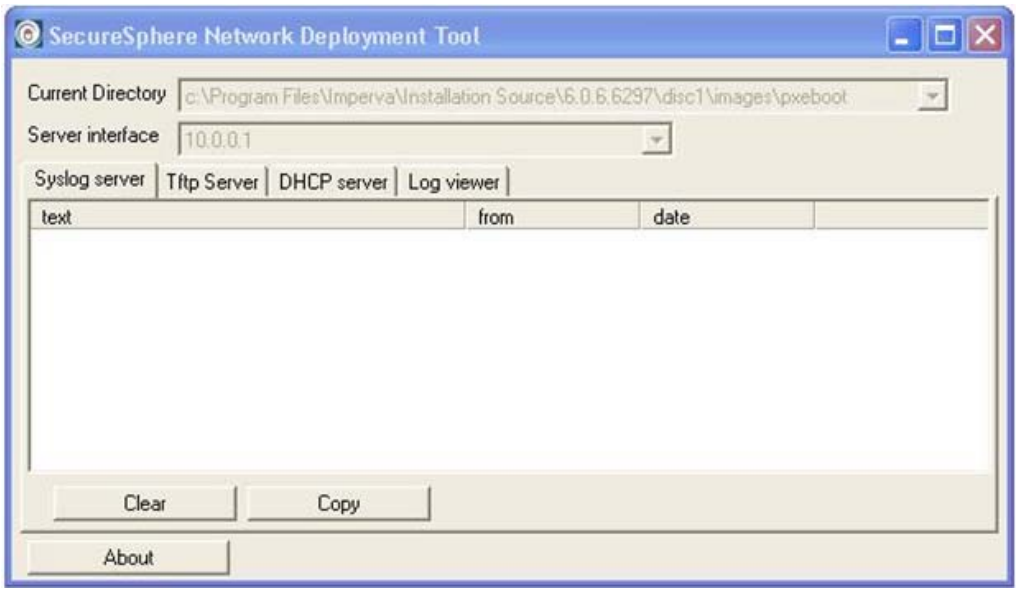


Figure 80 Network Deployment Tool

Note: Interaction With Windows Firewall and other Personal Firewalls: The network deployment tools require access to the network. It requires both that you allow connection to and from it, as well as opening network connections from the host. When the application is first launched, Windows Firewall pops up the following two messages:



3. Click **Unblock** in both pop-ups. Other firewalls may contain additional required configurations.

Booting the Target Appliance

This section contains instructions for booting and installing SecureSphere software from the network for the following appliances:

- G2 and G2-2 Target Appliance on page 380
- G-series Target Appliance (not a G2 or G2-2) on page 381
- M-series or X-series Target Appliance on page 381

G2 and G2-2 Target Appliance

To boot and install SecureSphere software from the network on a G2 or G2-2 target appliance:

1. Connect a VGA or serial console to the appliance, so that you will be able to monitor the progress of the installation.

   The instructions for doing this are in the ***Quick Start Guide*** for the appliance.

2. Turn on the appliance.

   Out of the box, a G2 or G2-2 appliance attempts to boot from the network upon startup (using its LAN3 interface, see Connecting the Target Appliance and Deployment Server on page 378). When the appliance starts, it automatically attempts to boot from the network. If the BIOS settings were modified, see Reconfiguring the G2 and G2-2 Appliance Not to Boot from the Network on page 383.

3. When the deployment server on the network is successfully discovered, the boot menu is displayed on the console:

```
Welcome to IMPERVA SecureSphere 9.0 Installation
--------------------------------------------------------------------------------
This action performs a clean installation of the appliance software. The
contents of the appliance's disk will be erased. This action cannot be undone.

The device will reboot from the local HDD if no action is specified within 30
seconds.

Choose one of the following actions and then press <ENTER>:

install - By default installation output is sent to the VGA and appears in the
network deployment tool. This command accepts additional parameters to redirect
the output (see the Administration Guide for further details). To install the
specified build 9.0 type: install

installserial - By default installation output is sent to ttyS1 (serial
output).To install 9.0 and send the output to ttyS0, type: installserial

local - The appliance software is not installed and the disk is not erased. To
boot from the local installed version, wait 30 seconds or type: local
```

Figure 81 Boot Menu

4. Enter one of the following commands:

To ...	Enter the following text and then press <Enter>
install from the network with output to a VGA monitor	`install`
install from the network with output to a serial console	`installserial`
boot from the currently installed version **Note:** In this case the hard disk is not erased.	`local` (or alternatively, wait 30 seconds)

G-series Target Appliance (not a G2 or G2-2)

To boot and install SecureSphere software from the network on a G-series target appliance (not a G2 or G2-2):

1. Connect a VGA or serial console to the appliance, so that you will be able to monitor the progress of the installation.

   The instructions for doing this are in the ***Quick Start Guide*** for the appliance.
2. Turn on the appliance.
3. When the appliance boots, you are prompted to press <F12> to boot from the network.
4. When the deployment server on the network is successfully discovered, the boot menu (Figure 81 on page 380) is displayed on the console:
5. Enter one of the following commands:

To ...	Enter the following text and then press <Enter>
install with output to a VGA monitor	`install`
install with output to a serial console	`installserial`

M-series or X-series Target Appliance

To boot and install SecureSphere software from the network on an M-series or X-series appliance:

1. Connect a serial console to the appliance, so that you will be able to monitor the progress of the installation.



Note: For backward-compatibility reasons, the installation procedure outputs to a VGA port by default. Because the X and M appliances do not have a VGA port, you must connect a serial console in order to monitor the installation.

   The instructions for doing this are in the ***Quick Start Guide*** for the appliance.
2. Turn on the appliance.
3. When the appliance boots, you are prompted to press **L** to boot from the network.
4. When the deployment server on the network is successfully discovered, the boot menu (Figure 81 on page 380) is displayed on the serial console:

5. Enter the following command:

To ...	Enter the following text and then press <Enter>
install from the network with output to a serial console	`install console=ttyS0,38400`

Monitoring Installation Progress

Monitoring installation progress is done from the Network Deployment Tool window (see Network Deployment Tool on page 379).

SecureSphere installation is divided into five stages.

To install SecureSphere:

1. PXE boot: the appliance receives a network address through DHCP.
2. The appliance downloads the code over TFTP, and executes the installation code.
3. Installation of the core operating system (Formatting the disk, installing Linux packages, and so on).
4. Installation of SecureSphere specific packages (Oracle, Kernel, and so on).
5. Post installation adjustments.
6. To monitor step 1, select the DHCP tab in the deployment program. The MAC and obtained IP of the appliance appear.
7. To monitor step 2, select the TFTP Server tab in the deployment program.
8. To monitor stages 3-5, select the Syslog Server tab. Installation progress messages are routed into the display.

When the installation is completed, the following line is displayed:

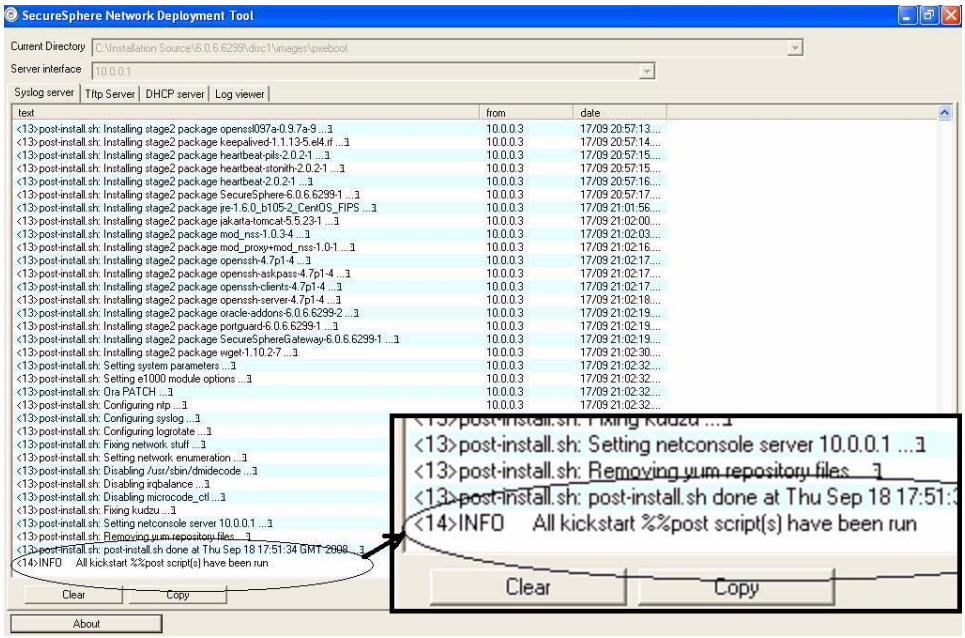


Figure 82 Monitoring installation progress

Finalizing Installation

Once the SecureSphere installation is complete, you need to finalize the installation:

- Connecting the management interface to the network
- Performing first time login and setting up network parameters.

These items are covered in detail in the Quick Start Guide of your specific appliance.

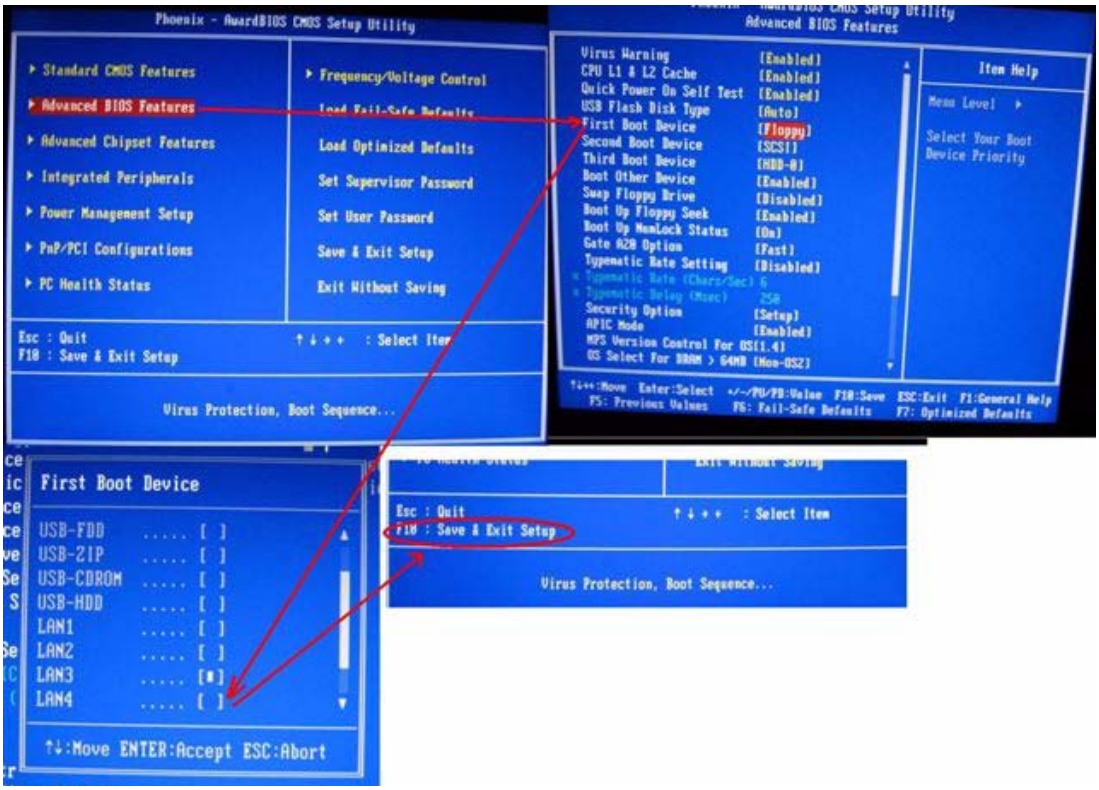
Reconfiguring the G2 and G2-2 Appliance Not to Boot from the Network

Out of the box, G2 and G2-2 appliances are configured to boot from the network (LAN3 - see Connecting the Target Appliance and Deployment Server on page 378). In most cases, this is harmless, as most DHCP servers (such as RIS) require manual intervention to perform network installation.

To make sure this does not happen (as well as decrease boot time), you can control whether the G2 boots from the network by changing the BIOS settings.

To change the BIOS settings when the appliance boots:

1. Press **<Del>** to enter the **BIOS** configuration screen.
2. Select **First Boot Device**.
3. Select **USB-HDD** (or any other option that is not LAN) and press **<Enter>**.
4. Press **<Esc>**.
5. Press **<F10>** to Escape & Exit.



Frequently Asked Questions

Can I deploy several appliances at once?

Yes. To do that, you must connect several machines to the same management interface on the deployment server, either using a hub or switch. Make sure that this network does not have any other DHCP server besides the deployment server.

Can I use network deployment to upgrade my appliance?

No. The installation will install the system from scratch, removing the previous version completely.

Can I perform the network installation process with only a keyboard connected to the appliance?

Yes. You boot the appliance (Booting the Target Appliance on page 380) without a monitor. You can monitor the installation progress through the dialog shown in Monitoring Installation Progress on page 382.

Serial Console Installation

1. If the appliance uses the serial console, add the required `console=` argument, for example:

```
boot: install console=ttyS0,38400
```

APPENDIX B

Network Services

This appendix describes various network configuration issues related to deploying SecureSphere, and includes:

- SecureSphere Component Communication on page 386
- Serial Console Access to SecureSphere on page 388

SecureSphere Component Communication

Table lists the protocols through which the various SecureSphere components communicate with each other.

SecureSphere Component Communication

Source	Destination	Protocol	Destination Port	Remarks
gateway	MX	HTTP	TCP 8083	If the gateway and MX server have a dedicated network (either with a cross cable or through a dedicated switch) then there is no need to open these ports on the firewall.
MX	gateway	SSH	TCP 22	
MX	gateway	HTTPS	TCP 443	
MX	www.imperva.com	HTTP	TCP 80	automatic signature update
gateway	syslog server	syslog	UDP 514	if audit is configured
MX	syslog server	syslog	UDP 514	
desktop	MX	HTTPS	TCP 8083	
desktop	MX	SSH	TCP 22	
gateway	DNS server	DNS	TCP 53 UDP 53	DNS is required to resolve host names defined in SecureSphere policies.
gateway	NTP server	NTP	UDP 123	NTP is needed to guarantee accuracy of timestamps.

Configuring Firewall Ports

The SecureSphere allows a great deal of flexibility in its deployment modes. Firewalls can be placed wherever they are required.

Figure 83 shows that ports that need to be open to enable different functions required by SecureSphere to communicate through the deployed firewalls.

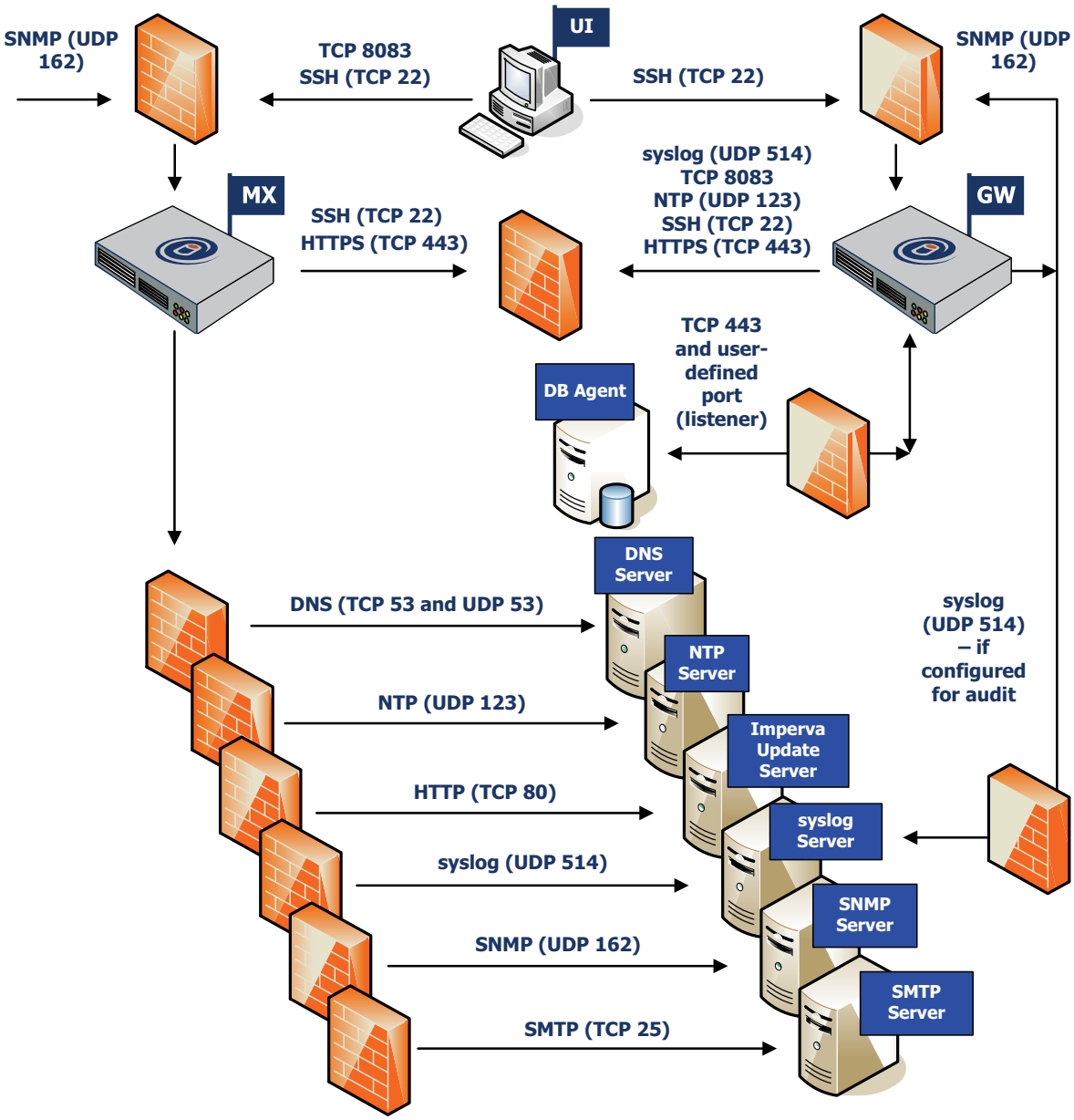


Figure 83 Firewall Port Configuration

Serial Console Access to SecureSphere

This section describes the steps administrators need to take in order interact with SecureSphere's Command Line Interfaces (CLIs) through a serial console, rather than a VGA and PS2 keyboard.

Supported Versions and Upgrades

Hardware

The steps described in this document are supported only on the FTL versions of G4, G8, G16 and MX appliances, with BIOS versions 74 and 85.

Software

The minimum SecureSphere software version required is 6.0.6.6302. Prior versions are not supported.

Upgrades

The changes described in this document will survive an upgrade from SecureSphere release 6.0.6.6302 to 6.2.0.6442. Other upgrades have not been tested. Furthermore, whenever SecureSphere is reinstalled, administrators must reapply the `grub.conf` changes described in Editing the GRUB Configuration File on page 390.

Supported Serial Console Settings

Throughout this document, the serial console settings administrators should use are as follows:

Serial Console Settings

Setting	Value
baud rate	38400
data bits	8
parity	none
stop bits	1
flow control	none
terminal emulation	VT 100+

VT 100 Escape Sequences

VT 100 key	Escape sequence sent
HOME	<ESC> h
END	<ESC> k
INSERT	<ESC> +
DELETE	<ESC> -

VT 100 Escape Sequences

VT 100 key	Escape sequence sent
PAGE UP	<ESC> ?
PAGE DOWN	<ESC> /
ALT	<ESC> ^A
CONTROL	<ESC> ^C
F1	<ESC> 1
F2	<ESC> 2
F3	<ESC> 3
F4	<ESC> 4
F5	<ESC> 5
F6	<ESC> 6
F7	<ESC> 7
F8	<ESC> 8
F9	<ESC> 9
F10	<ESC> 0
F11	<ESC> !
F12	<ESC> @

Before You Begin: Checking OS Layer Serial Console Access

In its default configuration, SecureSphere supports OS layer access via a serial console. It is highly recommended to first confirm that they you such access as follows:

1. Set the connections parameters on the console client (for example, using `putty`) to those defined in Table .
2. Connect to the SecureSphere appliance via its DB9 serial port.
3. Initialize the connection and confirm that you get a Linux prompt and are able to log in, for example, with the “secure” user credentials.



Note: If serial console access only at the OS layer is sufficient for your needs, then no configuration changes are needed.

Configuring BIOS Settings for Serial Console

After making the changes described below and rebooting the machine, you will be able interact with the BIOS UI though both the VGA and the serial console.

Use your existing VGA port and PS2 keyboard to make the following changes:

1. Power on the SecureSphere appliance.
2. Press F2 to enter BIO configuration

3. Set Server Management-> Console Redirection-> Console Redirection to one of the following:
   - [Serial Port A] (DB9)
   - [Serial Port B] (Rj45)
4. Set Flow Control to [None].
5. Set Baud Rate to [38.4K].
6. Set Terminal Type to [VT100+].
7. Set Legacy OS Redirection to [Enable].
8. Save & Exit using “F10”.

At this stage the Keyboard and VGA are no loner required.

Editing the GRUB Configuration File

Changing the settings below will allow you to interact with the bootloader and see the messages it prints to the console as modules are loaded.



Warning: Once these settings take effect, boot time messages will only be available through the serial console and not through the VGA console. Only BIOS and OS access will still be available through the VGA and PS2 keyboard.

1. Edit the `/boot/grub/grub.conf` file.
2. Add the following text at the end of each line that start with the word “kernel”:

   `console=ttyS0,38400`
3. Save the file and exit.

The `/boot/grub/grub.conf` file should now look like this (the added text is highlighted):

```
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this file
# NOTICE:  You have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /boot/, eg.
#          root (hd0,0)
#          kernel /vmlinuz-version ro root=/dev/sysvg/root.vol
#          initrd /initrd-version.img
#boot=/dev/sda
default=0
timeout=5
serial --unit=0 --speed=38400
terminal --timeout=5 serial console
title CentOS (2.6.18-53.1.4.el5.imp40smp)
        root (hd0,0)
       kernel /vmlinuz-2.6.18-53.1.4.el5.imp40smp ro root=/dev/sysvg/root.vol
rhgb quiet panic=10 console=ttyS0,38400
        initrd /initrd-2.6.18-53.1.4.el5.imp40smp.img
title CentOS (2.6.18-53.el5)
        root (hd0,0)
        kernel /vmlinuz-2.6.18-53.el5 ro root=/dev/sysvg/root.vol rhgb quiet
panic=10 console=ttyS0,38400
        initrd /initrd-2.6.18-53.el5.img
```

SecureSphere Network Installation with Serial Console

Network installation under a serial console is almost identical to one done with VGA and keyboard, except that the PXE client must be explicitly configured to use the console.

To configure the PXE client to use the console:

1. From the console, press <ESC><@> to start the network install.
2. When the "`boot:`" prompt is displayed, enter the following command:

   ```
   install console=ttyS0,38400
   ```
3. The installation process starts and the ongoing messages are displayed on both the serial console and in the Imperva Network Deploy Utility.
4. After installation, the machine will reboot and the terminal prompt will prompt you with login.

APPENDIX C

SAP Configuration

This document describes issues related to SAP configuration in Imperva SecureSphere, including:

- Configuring the SecureSphere Gateway on page 393
- Universal User Tracking on page 394
- Monitoring SAP Transactions on page 395
- Database Table Groups on page 398

Configuring the SecureSphere Gateway

SAP applications access the database in a unique way, which requires that SecureSphere be configured appropriately.

To configure the SecureSphere gateway:

1. Edit (using a text editor) the file `/opt/SecureSphere/etc/hades.cfg` on the gateway as shown below.

SecureSphere build 6302 and higher	Change the value of the parameter `sql_max_template_events` to 500. Change the value of the parameter `protocol_blocks_size0` to 12300.
SecureSphere builds prior to 6302	Change the value of the parameter `sql_max_saved_events` to 500. Change the value of the parameter `protocol_blocks_size0` to 12300.

2. Restart the SecureSphere gateway using the following command:

```
impctl gateway restart
```

Universal User Tracking

SecureSphere's Universal User Tracking (UUT) feature enhances security and auditing by analyzing traffic to accurately associate application front end users with applications and database queries. User identification is provided in alerts and audit reports, and security policies to restrict access to sensitive databases can be enabled on a per-user basis.

SecureSphere includes a default SAP UUT policy object which enables SQL Connection User Tracking for SAP, which you must apply to the relevant services.

For more information on how to do this, see the Universal User Tracking chapter in the ***SecureSphere User Guide***.



Note: The following SAP ECC versions are supported by default: 4.6, 4.7, 5.0, 6.0.

Monitoring SAP Transactions

SAP includes many thousands of pre-defined transactions, each of which defines a logical business unit of work, to accomplish specific tasks. SAP DBA's, programmers, users and auditors are accustomed to working at the transaction level rather than at the SQL statement level, and need to monitor, track and audit SAP applications at the SAP transaction level.

In addition to the option of monitoring SAP applications at the level of SQL statement, Imperva SecureSphere monitors SAP applications at the level of SAP transactions, enabling SAP administrators to audit SAP transaction activity directly.

Monitoring an application requires the ability to perform the following tasks:

Monitoring Task Overview

Task Overview	Description	For more information, see...
Define events of interest, that is, the events to be monitored.	Imperva's ADC Insights has compiled a list of sensitive SAP transactions, that is, transactions which access sensitive data such as user roles and authorizations, system monitoring, auditing *etc*. Users can also define additional SAP transactions to be tracked.	Defining SAP Transactions on page 396
Identify these events as they occur.	Two pre-defined audit policies audit these SAP transactions, and users can edit these policies and define new ones.	
React to the events: audit, alert, report, *etc*	Administrators can define reports based on the collected audit data.	Chapter 3, Reporting in ***SecureSphere User Guide***

Defining SAP Transactions

Imperva's ADC Insights provides a list of sensitive SAP transactions, defined in SecureSphere as elements of a privileged operations group.

SecureSphere administrators cannot make changes to this list, but they can add SAP transactions to the User Defined Privileged Operations Group and include these transactions in auditing and reporting.

Configuring SAP Transactions for use in SecureSphere

Because SecureSphere uses the privileged operations mechanism to identify SAP transactions, you must create a data enrichment policy to extract the SAP transactions from the SQL which is then recognized by SecureSphere as a privileged operation.



Note: This solution applies to SAP ECC 6.0.

The following table lists the main tasks that need to be conducted to configure SAP Transactions for use in SecureSphere

	Action	Description	For more information, see...
1	Configure a Data Enrichment Policy	Define a Data Enrichment policy to extract SAP Literals from SQL	Configure Data Enrichment Policy for SAP Transaction Detection on page 396
2	Define an Audit Policy	Define an audit policy that will only audit the transactions defined using the data enrichment policy	Configure an Audit Policy for Auditing SAP Transactions on page 397.
3	View audited transactions	Configure an audit view to display SAP transactions and save it as a report for future reference.	Viewing SAP Transactions in Audit on page 397

Configure Data Enrichment Policy for SAP Transaction Detection

To configure a Data Enrichment Policy for SAP SQL Transactions:

1. In the **Main** workspace, click **Policies** > **Data Enrichment**.
2. In the **Create New Policy** window, click **New**, type a **Name**, and from **Type** select **DB Service Enrichment**, then click **Create**.
3. On the **Rules** tab, create a new **User Defined Field**, under **Target Field Name** type **SAP-T-Code**, select the **From Event SQL** extraction method, then click **Save**. The field becomes expandable.
4. Expand the item you just added, under **Extract Literal #**, type **3**, and in the **From Query** field, type:

   ```
   select "devclass" from "tadir" where "pgmid" = ? and "object" = ? and
   "obj_name" = ?
   ```
5. Expand the **Additional Conditions** option, in the **when Literal #** field, type **2**. In the second field after **is**, type **TRAN**.
6. In the **Apply to** tab, select the database service on which the SAP application is running, for example Oracle.
7. Click **Save**.

   Once you have completed configuring the data enrichment policy to extract the required fields, you need to configure an Audit policy to audit this traffic as described in Configure an Audit Policy for Auditing SAP Transactions on page 397.

Configure an Audit Policy for Auditing SAP Transactions

Once you have created a data enrichment policy to extract the literals needed to audit SAP transactions, you need to configure an audit policy.

To configure an Audit Policy to view SAP SQL extraction:

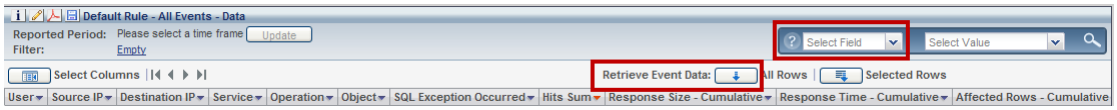
1. In the **Main** workspace, click **Policies** > **Audit**.
2. In the **Create New Policy** window, click **New**, type an intuitive **Name** such as SAP SQL Transactions, from **Type** select **Database**, then click **Create**.
3. On the **Match Criteria** tab, add the **Destinations Table** criteria by clicking its Green Arrow .
4. Expand the criteria and add the table **tadir**, to the selected pane.
5. On the **Match Criteria** tab, add the **Enrichment Data** criteria by clicking its Green Arrow .
6. Expand the criteria,
   - Under **User Defined Field** type **SAP-T-Code**
   - In the **Operation** field select **Exclude All**, and under **User Defined**, click new then type **TXX**. This tells the audit policy to filter only events with enrichment data on the SAP-T-Code field.
7. On the **Settings** tab, under **User Defined 1**, select **SAP-T-Code**.
8. In the **Apply** to tab, apply the policy to the appropriate SAP database server and save it.

Viewing SAP Transactions in Audit

Once you have configured a data enrichment policy to extract SAP data and an audit policy to audit this data, you can view SAP transactions in the audit window.

To view SAP transactions in the audit window:

1. In the **Main** workspace, click **Audit > DB Audit Data**.
2. In the **Views** pane, select the **Data** view.
3. In the upper right-hand corner of the main audit window, under **Select Field**, choose **User Defined 1**.



4. Select a row in the resulting data, then click **Retrieve Event Data**.
5. To save this view for easy access, click **Save as Report** .

Other Audit Policies

You can define additional audit policies for SAP transactions, using the “SAP - Transactions” audit policy as a model. However, you should note that if you add one of the individual SAP transactions listed under **Privileged Operations** to the **Selected** list, the individual SAP transaction will be audited twice, because “SAP Transaction” includes all SAP transactions. In this case, remove “SAP Transaction” from the **Selected** list.

Database Table Groups

For SAP, SecureSphere defines a number of Database Table Groups. For SAP versions prior to ECC 6.0 (4.6. 4.7 and 5.0), the tables relevant to each group have different names in SAP.



Note: The information given here relates to the default SAP configuration. If you changed table names during configuration, you must also modify these objects accordingly (see below).

If you are using one of these versions, you must:

1. Manually create a Database Table Group for this purpose.
2. Associate the Database Table Group with the SAP application.
3. Clone the different audit and security policies which use the Database Table Groups and replace those default Database Table Groups with the ones you have just created.

To manually create a Database Table Group for ECC 4.6, 4.7 and SAP 5.0:

1. In the **Main** workspace, select **Setup** > **Global Objects**.
2. Under **DB-Related Objects,** right-click on **Database Table Groups**.
3. Select **Create Database Table Group** from the menu.
4. In the **Create Database Table Group** window, enter a **Name**.
5. Select the relevant database services.

To associate the Database Table Group with the SAP application:

1. In the **Main** workspace, select **Setup** > **Sites**.
2. Navigate to the SAP application.
3. In the **Definitions** tab, add the Database Table Group.

For more information about these actions, see ***SecureSphere User Guide***.

APPENDIX D

Add-Ons

This appendix describes various network configuration issues related to configuring add-on hardware in conjunction with SecureSphere, and includes:

- Hardware Security Modules (HSM) on page 400
- Storage Area Networks (SAN) on page 422
- SSL Accelerator on page 433
- LOM (Lights Out Management) on page 434

Hardware Security Modules (HSM)

Hardware Security Module devices (HSMs) store private encryption keys in specialized key storage devices. These devices protect the key information by making it impossible to gain access to the keys, even if the device is stolen.

A network HSM (Hardware Security Module) device is a central key management server which stores private keys. The network HSM provides a service to other devices on the network for performing operations with the secret keys.

Imperva SecureSphere supports the use of the following HSMs:

- nCipher card: nCipher Card on page 400
- nCipher netHSM: nCipher netHSM on page 406
- SafeNet LunaSA: SafeNet LunaSA on page 411

All these solutions provide:

- secure storage of up to 128 private keys
- SSL acceleration

nCipher Card

The nCipher card is installed inside the SecureSphere appliance.

Installing the nCipher Card

The nCipher card is installed in an available PCI slot in the appliance.

To install the nCipher Card:

1. Shut down the appliance.
2. Power down the appliance.
3. Remove the appliance cover.
4. Insert the nCipher card into the PCI slot and verify that it is firmly in place.
5. Replace the cover.
6. Power on the appliance.

Installing the nCipher Card Driver

To install the nCipher card driver:

1. Execute the following command:

```
/opt/nfast/sbin/install
```

Verifying the Installation

To verify the nCipher card installation:

1. Execute the following command:

```
/opt/nfast/bin/enquiry
```

The output should resemble the following:

```
Server:
 enquiry reply flags  none
 enquiry reply level  Six
 serial number        EFEB-96AB-EBE3
 mode                 operational
 version              2.32.14
 speed index          4240
 rec. queue           390..590
 level one flags      Hardware HasTokens
 version string       2.32.14cam6, 2.22.43cam8 built on Oct 13 2006 16:16:12
 checked in           0000000046dee54e Wed Sep  5 20:20:14 2007
 level two flags      none
 max. write size      8192
 level three flags    KeyStorage
 level four flags     OrderlyClearUnit HasRTC HasNVRAM HasNSOPermsCmd ServerHasPollCmds
FastPollSlotList HasSEE HasKLF HasShareACL HasFeatureEnable HasFileOp HasPCIPush
HasKernelInterface HasLongJobs ServerHasLongJobs AESModuleKeys NTokenCmds
JobFragmentation LongJobsPreferred Type2Smartcard
 module type code     0
 product name         nFast server
 device name
 EnquirySix version   4
 impath kx groups
 feature ctrl flags   none
 features enabled     none
 version serial       0
 remote server port   9004
Module #1:
 enquiry reply flags  Failed
 enquiry reply level  Six
 serial number        EFEB-96AB-EBE3
 mode                 operational
 version              2.22.43
 speed index          4240
 rec. queue           35..152
 level one flags      Hardware HasTokens
 version string       2.22.43cam8 built on Oct 13 2006 16:16:12
 checked in           00000000452f6a4d Fri Oct 13 12:28:29 2006
 level two flags      none
 max. write size      8192
 level three flags    KeyStorage
 level four flags     OrderlyClearUnit HasRTC HasNVRAM HasNSOPermsCmd ServerHasPollCmds
FastPollSlotList HasSEE HasKLF HasShareACL HasFeatureEnable HasFileOp HasPCIPush
HasKernelInterface HasLongJobs ServerHasLongJobs AESModuleKeys NTokenCmds
JobFragmentation LongJobsPreferred Type2Smartcard
 module type code     7
 product name         nC1003P/nC3023P/nC3033P
 device name          #1 nFast PCI device, bus 13, slot 1.
 EnquirySix version   5
 impath kx groups     DHPrime1024
 feature ctrl flags   LongTerm
 features enabled     StandardKM ModexpSpeedRating
 version serial       24
 rec. LongJobs queue  34
 SEE machine type     PowerPCSXF
```

Figure 84 nCipher enquiry command sample output

From the above sample output, you can see the following:

- The nfast server is up and its mode is operational ("`mode`" is "`operational`").
- One HSM was detected, at PCI location 13:01 (bus 13, slot 1).
- The HSM mode is operational.

Security World Initialization

The nCipher security world must be initialized whenever one or more of the following conditions is true:

1. The HSM is newly installed, so it does not yet have a security world.
2. An existing security world is discarded.
3. Whenever the appliance is reinstalled.

To initialize the security world:

1. On the card's bracket, move the switch to the **I** position (initialization).

   On G series appliances, the bracket is accessible from the rear.

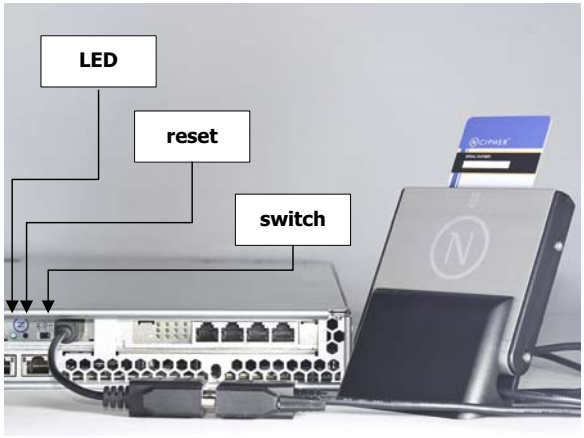


Figure 85 HSM Card Bracket and Reader - G Series Appliances

On X series appliances, the bracket is accessible from the front.

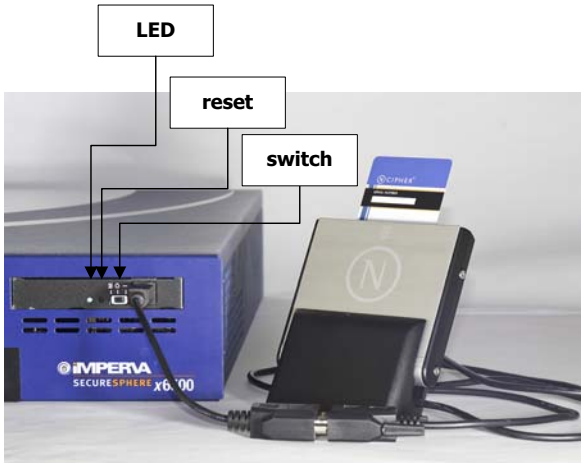


Figure 86 HSM Card Bracket and Reader - X Series Appliances

2. Press the RESET button (use a paper clip).

   The LED will blink for a few seconds.
3. When the LED stops blinking, use the nCipher `enquiry` command to confirm that the card is in the pre-initialization mode (see Figure 84), that is, that "`mode`" is "`pre-initialization`".

4. Execute the following command:

```
/opt/nfast/bin/new-world -i -Q 1/1
```

5. When you are asked to do so, insert the SmartCard into the nCipher reader.
6. When you are asked for a passphrase, press <Enter>.

   The output should resemble the following:

```
[root@Nigiri bin]# /opt/nfast/bin/new-world -i -Q 1/1
11:43:11 WARNING: Module #1: preemptively erasing module to see its slots!
Create Security World:
 Module 1: 0 cards of 1 written
 Module 1 slot 0: unknown card
 Module 1 slot 0:- no passphrase specified - overwriting card
Card writing complete.
security world generated on module #0; hknso =
b9d79789b3386f58e0c150f7f3f0657a976e036c
```

7. When the LED stops blinking, use the nCipher **`enquiry`** command to confirm that the card is now in the initialization mode (see Figure 84), that is, that "**`mode`**" is "**`initialization`**".
8. On the card's bracket, move the switch to the **O** position (operational).
9. Press the RESET button (use a paper clip).

   The LED will blink for a few seconds and then will remain mostly on, that is, it will blink only every few seconds.
10. At this point, use the nCipher **`enquiry`** command to confirm that the card is in the operational mode (see Figure 84), that is, that "**`mode`**" is "**`operational`**".
11. Execute the following command:

```
/opt/nfast/bin/cryptest
```

    The card will run some internal tests.
12. Confirm that the internal tests were successful by reviewing the output.

    At the end of the output, a message summarizes the number of tests run and their results. For example:

```
...
...
...
16 key types OK, 6 types and 1 mechanisms skipped, 54 mechanisms successfully
tested
```

13. At this point, you can remove the SmartCard from the card reader.

Importing Keys

This section provides an overview of the process. For detailed information on how to do this, see the nCipher documentation.

This procedure will import one or more keys into the HSM.

14. Obtain the protected server's certificate as a **`<name>.pfx`** file.

    For example, assume the server uses **`newkey.pfx.`** This file contains both the server's private key and its certificate.

You will:

- Extract the key and certificate into two separate files.
- Import the key into the HSM and make a “fake” key.
- Upload the fake key and certificate to the SecureSphere management server.

15. The private key imported into HSM must be unencrypted. To create a file containing the key and certificate without the passphrase, execute the following command:

```
openssl pkcs12 -in newkey.pfx -out newkey-combined.pem -nodes
```

For example:

```
[root]# openssl pkcs12 -in newkey.pfx -out newkey-combined.pem
-nodes
Enter Import Password:  **********
MAC verified OK
```

16. You now have a text file named **newkey-combined.pem** (in the above example), which includes two keys. Next, you will create other two text files from this file:
    - one for the key
    - one for the certificate

    16.1 Execute the following command:

```
cp new-combined.pem newkey-private.pem
```

    16.2 Using a text editor such as **vi**, delete from **newkey-private.pem** all the lines except for the following:

```
-----BEGIN RSA PRIVATE KEY-----
……
…
-----END RSA PRIVATE KEY-----
```

`newkey-private.pem` now contains only the private key.

16.3 Save `newkey-private.pem`.

16.4 Execute the following command:

```
cp new-combined.pem newkey-cert.pem
```

16.5 Using a text editor such as `vi`, delete from `newkey-cert.pem` all the lines except for the following:

```
-----BEGIN CERTIFICATE-----
……
……
-----END CERTIFICATE-----
```

`newkey-cert.pem` now contains only the certificate.

16.6 Save `newkey-cert.pem`.

17. Execute the following command:

```
/opt/nfast/bin/generatekey --import embed protect=module \
pemreadfile=newkey-private.pem embedsavefile=fake-newkey-private.pem \
plainname=newkey nvram=no
```

For example:

```
[root]# /opt/nfast/bin/generatekey --import embed protect=module \
pemreadfile=new-private.pem embedsavefile=fake_new_private.pem \
plainname=new nvram=no
Key successfully imported.
Path to key: /opt/nfast/kmdata/local/
key_embed_b671fd72759d086ad980f010fd853c4e2eeacece
```

18. Using a disk-on-key or some other media, carry the following files (created in the previous step) to the computer from which you run the SecureSphere GUI (the file names from the example above are given here):
    - `newkey-cert.pem`
    - `fake_newkey_private.pem`



Warning: These files contain the server's private key in unencrypted form. You must erase this extremely sensitive information in accordance with your site's procedures.

Update the Gateway HSM

19. On the SecureSphere gateway, start `impcfg`.
20. Select **Manage SecureSphere Gateway** > **Manage hardware security modules (HSM)** > **Enable nCipher HSM**.
21. **Apply** and **Confirm** the operation.

Update the Server with the Certificate Key

This section provides an overview of the process. For detailed information on how to do this, see the ***SecureSphere User Guide***.

22. Start the SecureSphere GUI.
23. Got to **Setup** > **Sites**, select (or create) an HTTP service.
24. In the HTTP service's **Definitions** tab, unnder **Encryption Support**, click  .
25. In the **Add SSL Keys** window:
    25.1 Enter a **Name**.
    25.2 Check **HSM**.
    25.3 Select **PEM file format**.
    25.4 In **Private Key**, browse to the `fake-newkey-private.pem` file.
    25.5 In **Public Key**, browse to the `newkey-cert.pem` file.
    25.6 click **Upload**.

nCipher netHSM

This section includes the following:

High Level Functional Description on page 406
Components Taking Part in the Integration on page 406
High Level Installation Process on page 407
nCipher HSM Installation on page 407
Setting Up the Integration on page 408
Basic netHSM Configuration on page 409

High Level Functional Description

This section describes the integration with the network HSM provided by the nCipher company, netHSM.

- SecureSphere supports storing keys on the netHSM and accessing the keys in real-time in order to decrypt SSL web traffic. The following options are supported:
- Accessing multiple keys from multiple SecureSphere gateways.
- Accessing the same key from multiple SecureSphere gateways, including the case of gateways that are in high availability mode.
- Working with a mix of keys, where some keys are stored in an HSM device while other keys are stored in SecureSphere.



Note:
- When generating command state, do not use passphrase.
- If the key is already in nCipher, then you must create a fake key using the `generate -r embed` command.

Components Taking Part in the Integration

The following components are involved in the integration:

- The **nCipher netHSM** – the server that holds the secret keys (referred to in this document as the **netHSM)**.
- The **nCipher RFS Server** – the remote file system server (referred to in this document as the **RFS Server**).
- The **SecureSphere gateway** – performs the traffic decryption and receives key services from the netHSM. The SecureSphere gateway will be referred to in this document as the **gateway**.
- The **SecureSphere MX Server** – holds the security policy instructing which keys should be applied to the encrypted traffic. The SecureSphere MX Server will be referred to in this document as the **MX Server**.

High Level Installation Process

To integrate SecureSphere to the netHSM, proceed as follows:

1. Register the gateway to the netHSM.
2. Register the gateway to the RFS Server.
3. Enable nCipher support on the SecureSphere gateway.
4. Synchronize between the gateway and the RFS server.
5. Define the security policy on the MX Server.

Figure 87 shows the relationship between the components which comprise an nCipher HSM configuration.

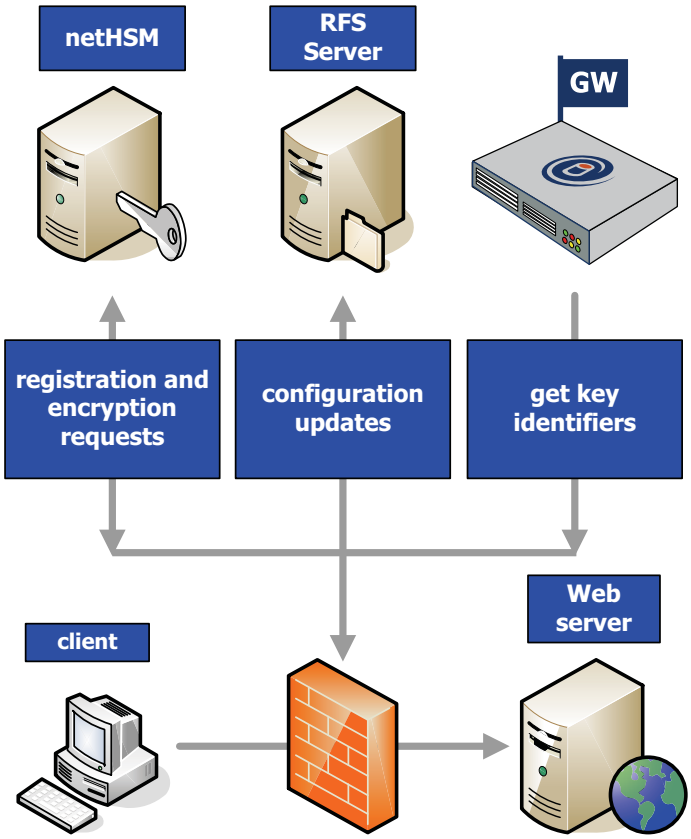


Figure 87 netHSM Components

nCipher HSM Installation

Assumptions

This section outlines the process of integrating SecureSphere with a netHSM. It is assumed that the netHSM is already functional, so what remains to be done is to integrate SecureSphere to the device.

Consult with your netHSM administrator to confirm that the following prerequisites have been met.

1. netHSM is operational, and that the security world of the HSM device is appropriately initialized.
2. The correct version of SecureSphere is already installed and has successfully gone through the setup process.

   netHSM integration is enabled in SecureSphere version 6.0.6 patch 5 and above.
3. Keys are loaded to the netHSM: the keys are already stored in the netHSM, and for each stored key you have the matching fake key and certificate. If you need to do this yourself, see Basic netHSM Configuration on page 409 for instructions.
4. The RFS server is already installed and you know its IP address.

Any gateway using netHSM should have network access to the RFS through its management interface.

5. All connections between the gateway and the netHSM and the RFS server pass through the gateway's management interface.

   It is assumed that you have network connectivity between the gateway and the RFS Server and the netHSM.

6. Confirm that you have access to the RFS Server and the netHSM.

   The RFS Server and the netHSM are separate devices (see Figure 87) under the responsibility of the netHSM administrator. Several steps in this procedure are performed on the nCipher machines. If you do not have access to these machines, please contact the nCipher administrator to obtain access.

Installing the nfast Software Package

To install the nCipher application:

1. Execute the following commands:

```
/opt/nfast/sbin/install
```

Setting Up the Integration

Per-installation Checklist

Before setting up the integration procedure between SecureSphere and the netHSM, review the following checklist:

DB Pre-installation checklist

Step	✓	Action
1		netHSM is operational
2		RFS server is operational
3		SecureSphere is operational
4		You have the netHSM IP address
5		You have the RFS Server IP address
6		nfast RPM is installed on the gateway

To integrate between SecureSphere and the netHSM:

1. Ensure that the SecureSphere gateway accesses the netHSM and to the RFS Server through the appliance's management interface.

   Do this in `impcfg` (**Manage Platform** > **Manage Networks** > **Static Routes**).

2. Define the gateway as a client to netHSM.

   On the **netHSM**, select **Menu** > **System** > **System configuration** > **Client config** > **New/Edit client** from the menu, and enter the gateway's management IP address.

3. On the SecureSphere gateway, get the netHSM's electronic serial number and key-hash (which will be used in subsequent commands) by executing the following command:

```
/opt/nfast/bin/anonkneti <netHSM-IP-address>
```

   You will get the following output: ESN KEY-HASH.

4. Register the gateway as a client to netHSM by executing the following command:

```
/opt/nfast/bin/nethsmenroll <netHSM-IP-address> <ESN> <KEY-HASH>
```

where **<ESN>** and **<HASH>** are the values obtained in the previous step.

5. Synchronize the gateway with the RFS Server as follows:

5.1 Add the gateway as a permitted entity on the RFS server by executing the following command on the RFS Server for each gateway:

```
/opt/nfast/bin/rfs-setup --gang-client --write-noauth <Gateway-IP-Address>
```

5.2 Bond and synchronize each gateway with the RFS Server by executing the following command on the gateway:

```
/opt/nfast/bin/rfs-sync --setup --no-authenticate <RFS-IP-address>
```

5.3 Update the secure world and certificates files by running the following command:

```
/opt/nfast/bin/rfs-sync --update
```

6. Enable nCipher support on the SecureSphere gateway as follows:

6.1 Run **impcfg** and enable HSM (**Manage SecureSphere Gateway** > **Manage hardware security modules (HSM)**).

6.2 In **impcfg**, apply the configuration.

6.3 Confirm that the private keys are already loaded to the netHSM.

It is assumed that the private keys are already loaded to the netHSM, and you have the appropriate fake keys, and matching certificates. If you still need to do this yourself, see Basic netHSM Configuration on page 409.

7. Configure the keys on the SecureSphere management server by editing the web service and adding the appropriate fake keys and matching certificate files.
8. Sign these keys as HSM keys by selecting **HSM** for these keys.

Once the gateway is updated, you can start decrypting traffic using your netHSM device.

Terminating the Integration

To terminate the integration between the netHSM and SecureSphere:

1. Remove the keys from the MX by deleting all the keys marked as HSM, and replacing them with the real keys as appropriate.
2. Disable the nCipher HSM by disabling HSM (**Manage SecureSphere Gateway** > **Manage hardware security modules (HSM)**)
3. On the gateway, remove the RPM by executing the following command:

```
#rpm –e nfast
```

Basic netHSM Configuration

You must import one or more keys into the netHSM.

1. Obtain the protected server's certificate as a **<name>.pfx** file.

   For example, assuming the server name is Lizard, the file name would be **lizard.pfx**. This file contains both the server's private key and its certificate.

2. Open the server's certificate file (for **lizard.pfx**) and extract the key and certificate (to a file named **lizard-combined.pem**) by running the following command:

```
openssl pkcs12 -in lizard.pfx -out lizard-combined.pem –nodes
```

3. Using a text editor such as **vi**, open the **lizard-combined.pem** file.
4. Separate the key and certificate out of the **lizard-combined.pem** file. into two separate files – one for the private key and the other for the certificate.
5. Save the lines between:

```
-----BEGIN RSA PRIVATE KEY-----
    and
-----END RSA PRIVATE KEY-----
```

   into a file named **lizard_private.pem.**

6. Save the lines between:

```
-----BEGIN CERTIFICATE-----
    ...
-----END CERTIFICATE-----
```

   into a file named **lizard_cert.pem**.

7. Import the key into the HSM and produce a fake key by executing the following command:

```
/opt/nfast/bin/generatekey --import embed protect=module \
pemreadfile=lizard_private.pem embedsavefile=fake_lizard_private.pem \
plainname=lizard nvram=no
```

   where:

   - **pemreadfile** is the real private key to be stored in the netHSM.
   - **embedsavefile** is the output fake key to be loaded on the MX Server.

8. Transfer the files **lizard_cert.pem** and **fake_lizard_private.pem** to the SecureSphere management server and import them.

   Make sure the **HSM** checkbox is checked.

9. After adding the key to the netHSM, synch it to the gateway by running the following command on the SecureSphere gateway:

```
/opt/nfast/bin/rfs-sync -update
```



Note: You must run the update command on the gateway every time you add or remove a key on the netHSM to be used on the gateway.

SafeNet LunaSA

This section includes the following:

High Level Functional Description on page 411
LunaSA Software Installation on page 412

High Level Functional Description

SafeNet LunaSA is a flexible, Ethernet-attached hardware security module (HSM) server offering powerful cryptographic acceleration, hardware key management, and multiple configuration profiles for applications where security and performance are a priority. Sensitive keys are created, stored, and used exclusively within the secure confines of the HSM to prevent compromise. LunaSA provides advanced features like direct hardware-to-hardware backup, split user role administration, multi-person authentication, and trusted path authentication.

The SecureSphere system interacts with the LunaSA using Open SSL.

LunaSA Highlights

- Keys are always in hardware - high assurance HSM.
- Ethernet-attached for easy deployment.
- Hardware key management and high-performance cryptographic acceleration.
- Secure remote administration and two-factor authentication.
- Accelerate multiple SSL Web servers - offload computationally intensive SSL connection setups from Web servers with LunaSA configured for shareable hardware SSL acceleration.



Note: When integrating SecureSphere with LunaSA, SecureSphere operates in non-FIPS compliant mode.

LunaSA High Level Installation Process

The LunaSA installation process consists of the following steps:

Install the LunaSA Package on the Gateway on page 412
Check the Network Connection Between the SecureSphere Gateway and LunaSA on page 413
Establish NTL Between the SecureSphere Gateway and LunaSA on page 413
Assign a Client (SecureSphere Gateway) to a LunaSA HSM Partition on page 416
Activate the Partition on page 417
Configure the SecureSphere Gateway on page 418
Edit /etc/Chrystoki.conf on page 419
Restart the SecureSphere Gateway on page 419
Create a Fake Key on page 420
Start the SecureSphere GUI. on page 420
De-Registering a LunaSA - Gateway Connection on page 421

LunaSA Software Installation

Install the LunaSA Package on the Gateway

1. Download the LunaSA **tar** file from the Imperva FTP site to the SecureSphere gateway, for example, to the **/tmp** directory.

	Location
32-bit	/Downloads/Tools/HSM/32Bit/
64-bit	/Downloads/Tools/HSM/64Bit/

2. Untar the file you downloaded by executing one of the following groups of commands (based on downloading the **tar** file to the **/tmp** directory):
   - For the 32-bit version of SecureSphere:

```
tar xvf luna-4.4.1-9-32bit.tar.bz2 -C /tmp
cd /tmp/luna_32bit
```

   - For the 64-bit version of SecureSphere:

```
tar xvf luna-4.4.1-9-64bit.tar.bz2 -C /tmp
cd /tmp/luna_64bit
```

3. Install the LunaSA package by executing the following command:

```
./install.sh
```

4. To the question "**Do you agree to the License contained in the product packaging?**", answer y.

```
IMPORTANT:  The terms and conditions of use outlined in the software
license agreement (Document #800230-002) shipped with the product
("License") constitute a legal agreement between you and SafeNet Inc.
Incorporated.  Please read the License contained in the packaging of this
product in its entirety before installing this product.

Do you agree to the License contained in the product packaging?

If you select 'yes' or 'y' you agree to be bound by all the terms
and conditions set out in the License.

If you select 'no' or 'n', this product will not be installed.
```

5. To the question "**Would you like to install the Luna JSP for Luna SA? (y/n)**", answer n.

   If the installation is successful, a message to that effect will be displayed.

6. To the question "**Would you like to install the SDK for Luna SA? (y/n)**", answer n.

```
Installed configurator-4.3.0-10.i386.rpm
Checking for /etc/Chrystoki.conf.rpmsave
Using new /etc/Chrystoki.conf
/etc/Chrystoki.conf is up to date.
ldconfig: Cannot mmap file /usr/lib/libvmcfssl.so.

ldconfig: Cannot mmap file /usr/lib/libvmcf.so.

Installed libcryptoki-4.3.0-10.i386.rpm
Installed vtl-4.3.0-10.i386.rpm
Installed ckdemo-4.3.0-10.i386.rpm
Installed multitoken-4.3.0-10.i386.rpm
Installed salogin-4.3.0-10.i386.rpm
Installed ctp-4.3.0-10.i386.rpm
ldconfig: Cannot mmap file /usr/lib/libvmcfssl.so.

ldconfig: Cannot mmap file /usr/lib/libvmcf.so.

Installed libshim-4.3.0-10.i386.rpm
Installed lunacmu-4.3.0-10.i386.rpm
Would you like to install the Luna JSP for Luna SA? (y/n)
n
If you wish to install the Luna JSP for Luna SA at a later time, simply run install_lunajsp.sh in the javasp directory.

../../docs/readme.txt: No such file or directory

Installation of the Luna SA Client Software - Release 4.3.0-10 successful.

Would you like to install the SDK for Luna SA? (y/n)
n
If you wish to install the SDK for Luna SA at a later time, simply run install_lunasdk.sh in the SDK directory.
```

Check the Network Connection Between the SecureSphere Gateway and LunaSA

7. On the SecureSphere Gateway, execute the following command:

```
ping <LunaSA IP>
```

where **<LunaSA IP>** is the IP address of the LunaSA device.

Create a LunaSA HSM Partition

To create a LunaSA HSM partition:

1. Connect to the LunaSA and login as **admin**.
2. Execute the following command:

```
partition create -name <partition name> -password <password>
```

3. Display the partition's detail's by executing the following command:

```
partition show -partition <partition name>
```

Establish NTL Between the SecureSphere Gateway and LunaSA

The Network Trust Link (NTL) must be established between LunaSA device and SecureSphere Gateway. The NTL is the safe connection used to transfer communication and encrypted / decrypted information between the GW and the LunaSA.

4. On the SecureSphere Gateway, execute the following command:

```
cd /usr/lunasa/bin
```

5. Securely transfer the **server.pem** file (the real certificate of the protected server) from the LunaSA, using the supplied Chrysalis-ITS Transfer Program (**ctp**) utility.
6. On the gateway, execute the following command:

```
./ctp admin@<LunaSA IP>:server.pem .
```

Note: The period "." at the end of the command indicates that the resulting file should be placed in the current directory.

7. You will be asked to enter the LunaSA Administrator password.

```
[root@localhost bin]# ./ctp admin@10.1.4.211:server.pem .
The authenticity of host '10.1.4.211 (10.1.4.211)' can't be established.
RSA key fingerprint is 15:08:94:36:76:86:5e:1a:79:1a:dd:49:94:5c:63:70.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.1.4.211' (RSA) to the list of known hosts.
admin@10.1.4.211's password:
server.pem           100% |*****************************|   798       00:00
[root@localhost bin]#
```

8. Verify that the Server Certificate has arrived at the SecureSphere Gateway by executing the following command:

```
[root@localhost bin]# ls
```

The **server.pem** file should be among the files listed.

Note: Any time the IP or hostname of the Luna SA is changed (such as when moving from a pre-production environment), the client(s) that have previously connected via SSH will detect a mismatch in the Luna SA server certification information and warn you of potential security breach. In this case, you will need to remove that server's certificate information from the client's known host file found in: **/<user home dir>/.ssh/known_hosts2**
If this happens in a production environment, it could potentially be a security breach requiring investigation.
Similarly, when you first open a **ctp** or **ssh** link, you must accept the certificate.
You can check the fingerprint of the certificate by executing the following command:
lunash:> sysconf -fingerprint -ssh

9. Register the HSM server certificate to the SecureSphere Gateway (client) by executing the following commands to enable the SecureSphere Gateway to create a secure connection with the HSM (the server):

```
cd /usr/lunasa/bin
./vtl addServer -n <LunaSAhostname-or-IPaddress> -c server.pem
```

```
[root@localhost bin]# cd /usr/lunasa/bin/
[root@localhost bin]# ./vtl addServer -n 10.1.4.211 -c server.pem

New server 10.1.4.211 successfully added to server list.

[root@localhost bin]#
```

Note:
- You can use either the IP address, or if the SecureSphere Gateway is configured with DNS, the LunaSA name.
- The **vtl** command is not interactive. It is called from the command line or a shell prompt, completes its current task, and then exits back to the shell.

10. Create a certificate and a private key for the SecureSphere Gateway by executing the following commands:

```
cd /usr/lunasa/bin
./vtl createCert -n <SecureSphere Gateway IP>
```

```
[root@localhost bin]# cd /usr/lunasa/bin/
[root@localhost bin]# ./vtl createCert -n 10.1.3.173
Private Key created and written to: /usr/lunasa/cert/client/10.1.3.173Key.pem
Certificate created and written to: /usr/lunasa/cert/client/10.1.3.173.pem
[root@localhost bin]#
```

Note:

- Use the IP address of the SecureSphere Gateway, since the SecureSphere Gateway has no host name in the network. **"-n"** (name) is the only mandatory item, and must be the SecureSphere Gateway IP (or hostname). Additional optional parameters can be added.
- For full command syntax and description, see the Reference section of SafeNet LunaSA Help.

11. Export the SecureSphere Gateway certificate (created in the previous step) to the LunaSA by executing the following commands:

```
cd /usr/lunasa/bin
./ctp /usr/lunasa/cert/client/<SecureSphere_gateway_cert>.pem admin@<LUNASA
hostname-or-IP>:
```

```
[root@localhost bin]# ./ctp /usr/lunasa/cert/client/10.1.3.173.pem admin@10.
211:
admin@10.1.4.211's password:
10.1.3.173.pem       100% |*****************************|   810       00:00
[root@localhost bin]#
```

Note:

- The SecureSphere Gateway certificate is the same SecureSphere Gateway certificate created in the previous section (**<SecureSphere Gateway IP>.pem**).
- You must login with the admin account to the LunaSA, otherwise the SecureSphere Gateway certificate will not be registered correctly.
- The LunaSA's IP address is used as in most cases the SecureSphere Gateway is not configured with DNS.
- The "**:**" after the destination is required. Without the colon, the **ctp** command does not recognize the supplied destination as a remote server.
- The file uploaded to the HSM is automatically placed in the appropriate directory. Do not explicitly specify a directory as the destination.

12. Register the SecureSphere Gateway certificate to the HSM server.

    The SecureSphere Gateway certificate, which you have already securely transferred (using **ctp**) from the SecureSphere Gateway to the HSM Server, in previous sections, must be registered at the HSM Server.

    12.1 Using the **admin** ccount, cnnect to LunaSA with **ssh**.

```
ssh admin@<LunaSA IP>
```

    12.2 Execute the following command:

```
client -register -client <client's-name> -ip <SecureSphere gateway's IP>
```

```
[root@localhost bin]# ssh admin@10.1.4.211
admin@10.1.4.211's password:

Luna Command Line Shell v3.2.0-0  - (c) 2004 SafeNet, Inc. All rights reserve

[lunasa] lunash:>client -register -client medusaclient -ip 10.1.3.173

'client register' successful.

Command Result : 0 (Success)
[lunasa] lunash:>
```

    The client's name is defined by the user.

    12.3 You can verify that the SecureSphere Gateway is now registered with the LunaSA HSM by executing the following command:

```
client -list
```

    For full command syntax and description, see the Reference section of SafeNet LunaSA Help.

    After this registration the NTL connection is completely established.

Assign a Client (SecureSphere Gateway) to a LunaSA HSM Partition

To assign a client to a LunaSA HSM partition:

1. Connect to the LunaSA and login as **admin**.
2. Execute the following command:

```
client a -client <clientname> -partition <partition name>
```

```
[lunasa] lunash:>client a -client medusaclient -partition MishaTestPartition

'client assignPartition' successful.

Command Result : 0 (Success)
[lunasa] lunash:>
```



Note: This description assumes the LunaSA has already been configured, and the SecureSphere Gateway was added to the existing setup. The parameter **<partition name>** is the name of the HSM Partition that was created earlier, following the configuration of the HSM.

If this command fails, contact Imperva support.

3. Execute the following commands on the gateway:

```
cd /use/lunasa/bin
./vtl verify
```



This command verifies that the SecureSphere Gateway is registered to the LunaSA partition.

If you receive an error message, then some parts of the configuration have not been properly completed. You may have to revert and restart the process. Alternatively, you may wish to open the SafeNet Online Help and follow the more comprehensive configuration procedure. You can also contact Imperva support.

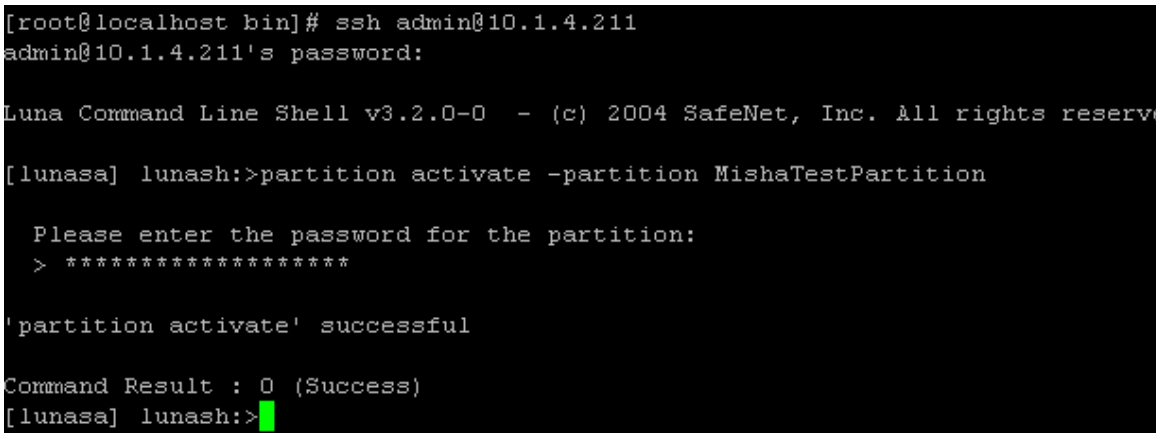
Activate the Partition

For a SecureSphere Gateway to use an HSM partition, without the need to enter a black key into the PED each time an HSM partition is used, activate the partition. To achieve this, an appropriate policy must be enabled for the partition.

To activate a partition:

1. Login to LunaSA as **admin**.
2. Execute the following command:

```
partition activate -partition <name>
```

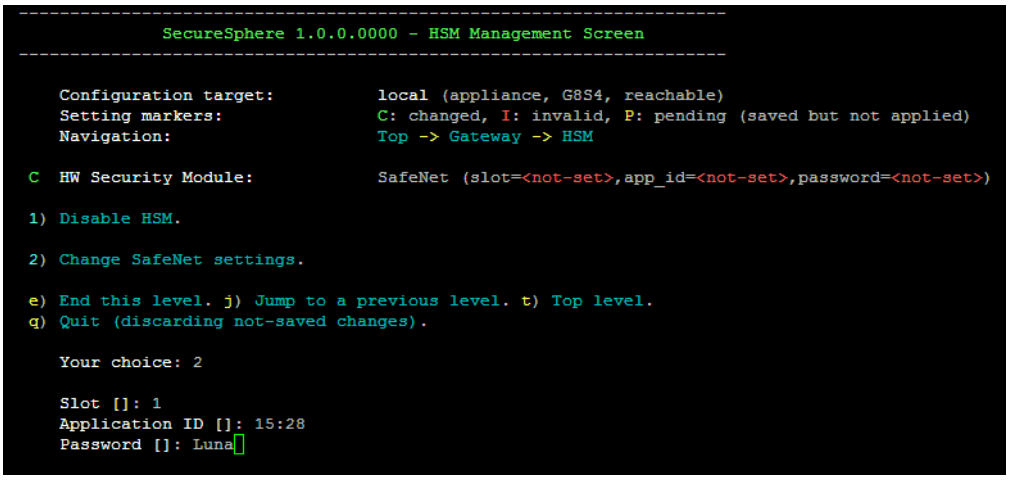


3. Enter the password for the partition (with the required dashes):
4. To initiate the activation, insert the LunaSA black key.
5. When you are instructed to, use the LunaSA PED to configure the LunaSA. It is possible that the LunaSA PED is turned off. If so, turn it on and follow the prompts on the screen. You will need the LunaSA black key as part of the process.
6. Enter the partition password when prompted.

Configure the SecureSphere Gateway

To configure the SecureSphere Gateway:

1. On the SecureSphere gateway, start `impcfg`.
2. From the **Top** screen, select **Manage SecureSphere Gateway**.
3. Select **Change hardware security modules (HSM)**.
4. Select **Enable SafeNet HSM**.
5. Select **Change SafeNet settings**.
6. Enable **netHSM**.
7. Set **Slot** to 1.
8. Set **Application** to a value of the form “XX:XX”.
9. Set **Password** to the partition password.



10. Save and exit.

Edit /etc/Chrystoki.conf

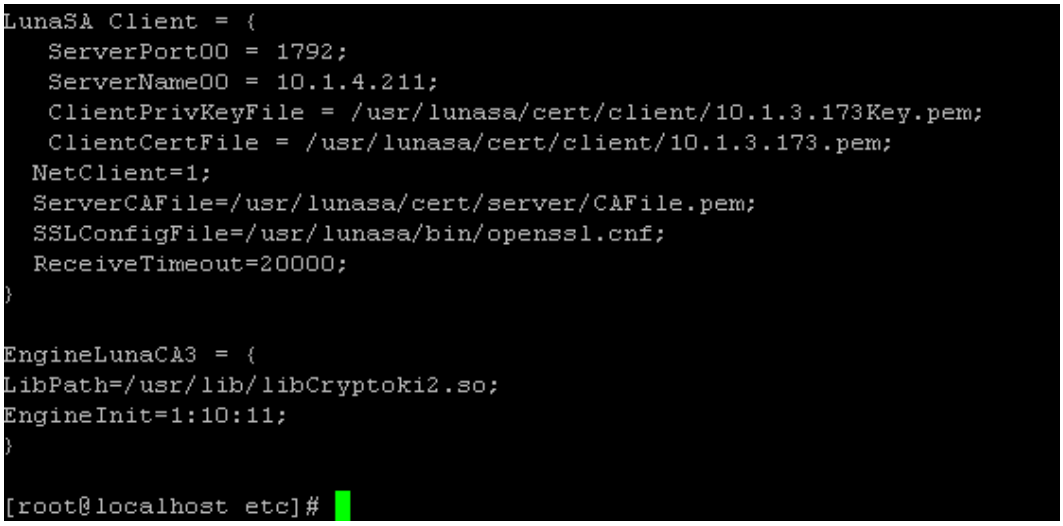
To edit the file `/etc/Chrystoki.conf`:

1. On the SecureSphere Gateway, open the **`/etc/Chrstoki.conf`** file with a text editor.
2. Add the following lines at the end of the file, *without indentations:*
   - For the 32-bit version of SecureSphere:

```
EngineLunaCA3 = {
LibPath=/usr/lib/libCryptoki2.so;
EngineInit=1:10:11;
}
```

   - For the 64-bit version of SecureSphere:

```
EngineLunaCA3 = {
LibPath64=/usr/lib/libCryptoki2_64.so;
EngineInit=1:10:11;
}
```



Restart the SecureSphere Gateway

1. Restart the SecureSphere Gateway.
2. Examine the **`gwlog`** file to verify that the SecureSphere Gateway is communciating with LunaSA by executing the following command:

```
gwlog | head -20
```

A notification similar to “HSM using SSL accelerator engine” indicates that the SecureSphere Gateway is communciating with LunaSA.

Export the Protected Server's Private Key to the LunaSA

1. On the SecureSphere gateway, execute the following command:

```
/usr/lunasa/bin/cmu importkey -in server-private-key.pem -keyalg RSA
```

The private key file must be a **.pem** file. If it is another file type, you can use the OpenSSL utility to convert it to a **.pem** file.

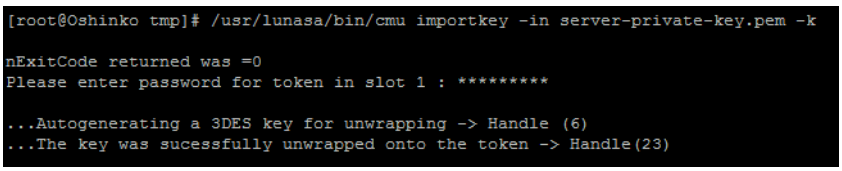


Figure 88 importkey command

This command returns the key's handle number in the Luna device. In the above example, this is **23**. You will need this number in the next step.

Create a Fake Key

1. On the SecureSphere gateway, execute one of the following commands:
   - For the 32-bit version of SecureSphere:

```
cp /tmp/luna_32bit/sautil /usr/bin/
/usr/bin/sautil -o -s 1 -i 1:1 -p '<password>' -a 0 -f fake_key.pem -c
```

   - For the 64-bit version of SecureSphere:

```
cp /tmp/luna_64bit/sautil /usr/bin/
/usr/bin/sautil -o -s 1 -i 1:1 -p '<password>' -a 0 -f fake_key.pem -c
```



Note: The password is the password of the partition.



Figure 89 sautil command

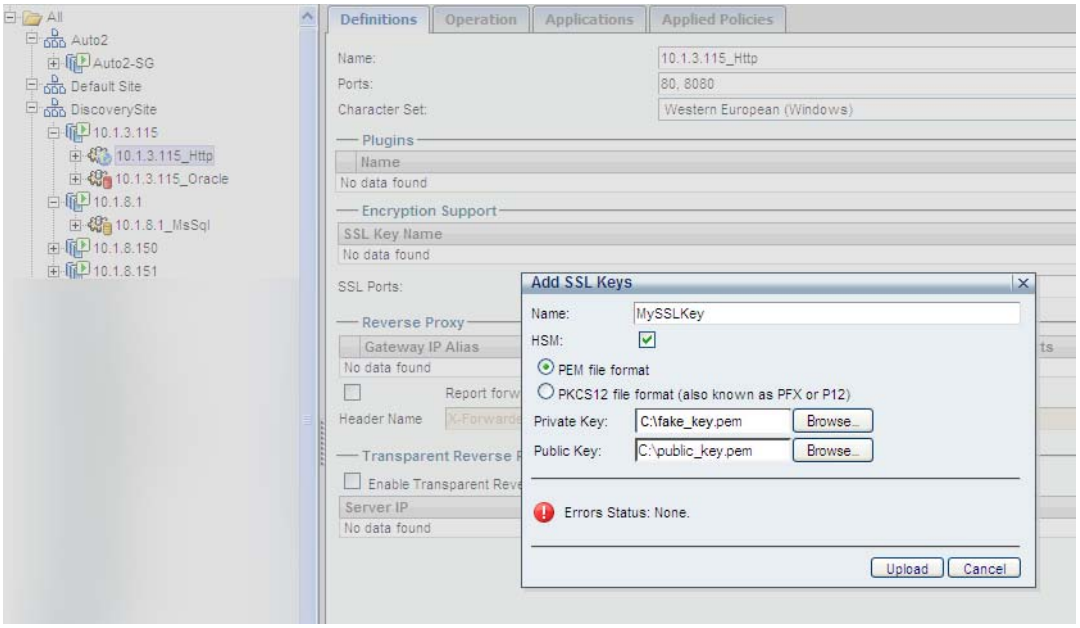
These commands open a connection to LunaSA (logs in to the partition) and let you choose a key (key handle, see the **importkey** command in the previous step) to export. In this example, the handle is **23**.

Once you select the relevant key, a fake key is then created and the connection is closed.

Next, you will load the fake key into SecureSphere.

2. Start the SecureSphere GUI.
3. In the **Main** workspace, click **Setup**.

4. In the **Sites** tree, select the HTTP service.
5. In the **Definitions** tab, under **Encryption Support**, add an SSL key.



6. In the **Add SSL Keys** window, enter the following parameters:
   6.1 Enter a **Name** for the SSL key.
   6.2 Enable **HSM**.
   6.3 Select **PEM file format**.
   6.4 For **Private Key** and **Public Key**, browse to the PEM files.
   - For the private key, use the fake key you created earlier (see Create a Fake Key on page 420).
   - For the public key, use the protected server's public key.
7. Click **Upload**.
8. Test the SSL connection.

De-Registering a LunaSA - Gateway Connection

If you have multiple LunaSAs connected to the gateway and you wish to de-register one of them, the process includes de-registration on the relevant LunaSA device, and then de-registration of that LunaSA on the SecureSphere gateway side.

A failure in the process will result in a "Broken pipe" error, which indicates an incomplete registration.

To delete the gateway client from the LunaSA:

1. Login to the LunaSA device and execute the following command:

```
client delete -client <clientname>
```

To de-register a LunaSA on the SecureSphere gateway:

1. Execute the following commands:

```
cd /usr/lunasa/bin
./vtl deleteServer -n <LunaSA IP>
```

Storage Area Networks (SAN)

This section describes how to integrate SecureSphere with Storage Area Networks, and includes:

- SAN Overview on page 422
- Supported SAN Hardware on page 422
- Configuring SecureSphere for SAN on page 423
- Disabling the SAN on page 431

SAN Overview

SAN connectivity enables SecureSphere to store data on centrally managed storage, providing the following benefits:

- better allocation and use of resources
- storage redundancy for higher availability
- central storage security management
- central backup/restore strategies

SecureSphere supports the following usage scenarios for a Storage Area Network (SAN):

- On a gateway, you can use the SAN to store audit data collected by the gateway.
- On a managment server (MX), you can use the SAN to store configuration, event, audit and report archives.
- On a Onebox, you can use the SAN to store audit data, configuration, event, audit and report archives.

The section describes how to connect and define and connect SecureSphere to the Storage Area Network, and how to configure SecureSphere to use the SAN.

Supported SAN Hardware

Host Bus Adapters

SecureSphere supports the following Emulex Host Bus Adapters:

- For PCI-X single channel: LP10000
- For PCI-X dual channel: LP10000DC
- For PCI-E single channel: LPe11000
- For PCI-E dual channel: LPe11002

These PCI-X HBA cards provide one 2GB Fibre Channel link with automatic 1GB downward compatibility. The PCI-E HBA cards provide one 4GB Fibre Channel link with automatic 1GB downward compatibility.

Other HBAs are not currently supported.

Cabling

The HBA provides one or two Fiber Channel port via an LC type optical connector. A suitable optical FC cable must be provided by the SecureSphere user. The type of the cable depends of the equipment to which it will be attached (RAID or a FC switch).

Configuring SecureSphere for SAN



Note:

- On a SecureSphere gateway, SAN is used only for the audit data. The path of the audit directory is defined in the `audit-base-path` attribute in the `bootstrap.xml` file.
- On a SecureSphere MX, SAN is used for archiving. The path of the archive directory is defined in the SecureSphere GUI.

SAN Configuration Task Overview

SAN Configuration Tasks

Step	✓	Action	For more information, see
1.		Determine your storage requirements.	Determine Storage Requirements on page 424
2.		Make a note of the original SCSI configuration. **Note:** This step is to be performed **only** by authorized Imperva personnel.	Make a Note of the Original SCSI Configuration on page 424
3.		Add the HBA to the SecureSphere appliance. **Note:** This step is to be performed **only** by authorized Imperva personnel.	Add the HBA to the SecureSphere Appliance on page 425
4.		Check that the HBA card is functioning properly.	Check the HBA Card on page 425
5.		Request that the Storage Manager add a Logical Volume.	Request that the Storage Manager Add a Logical Volume on page 426
6.		Physically connect to the SAN.	Physically Connect to the SAN on page 427
7.		Scan the Fiber Channel (FC).	Scan the Fibre Channel on page 427
8.		Update `/etc/modprobe.conf`.	Update /etc/modprobe.conf on page 428
9.		Create a file system on the SCSI target.	Create a File System on the SCSI Target on page 429
10.		Mount the new file system.	Mount the New File System on page 429
11.		Test the new file system.	Test the New File System on page 429
12.		Create a startup file.	Create a Startup File on page 429
13.		Reboot the SecureSphere appliance.	Reboot the Machine on page 431
14.		Configure SecureSphere to use the SAN.	Configure SecureSphere to Use the SAN on page 431

Each of these steps is explained in detail in the following sections.

Determine Storage Requirements

1. Determine the storage requirements, taking into account the following considerations.

   Accurately planning storage requirements requires some analysis. Some issues that influence the decision include:

   - special requirements of the SecureSphere site
   - capacity of the SAN storage device(s)
   - amount of traffic audited by the SecureSphere gateways and archived by the MX
   - accumulated experience with historical storage requirements at this site
   - projections of future storage requirements



Note: The Storage Manager must allocate a separate Logical Volume for each SecureSphere appliance which accesses external storage.

Make a Note of the Original SCSI Configuration



Warning: This step is to be performed **only** by authorized Imperva personnel.

The appliance may already have SCSI devices, specifically internal SCSI disks. You must take a note of the SCSI devices which have been recognized before you add the Fibre Channel adapter. This will allow you to know what SCSI devices will be added by the FC connection.

2. To see the list of SCSI devices, examine the **`/proc/partitions`** file.

   On a machine with local SCSI disks, the **`/proc/partitions`** file will be similar to the following:

```
[root@localhost ~]# cat /proc/partitions
major minor  #blocks  name

   8     0  244008960 sda
   8     1      56196 sda1
   8     2  243947025 sda2
 253     0   29360128 dm-0
 253     1  142802944 dm-1
 253     2   68616192 dm-2
 253     3    3145728 dm-3
```

   In this example, there are partitions on the **`sda`** SCSI drive (**`sda`** stands for SCSI disk **`a`**), indicating that the machine currently has only one SCSI disk.

   Make a note of ***all*** the SCSI disks (everything that starts with **`sd`**).

Add the HBA to the SecureSphere Appliance



Warning:
- This step is relevant **only** for G-series appliances. For X-series appliances, a SAN card can only be installed in the factory, and not at the customer site.
- If the HBA card has been installed by the appliance manufacturer, it is not necessary to perform this step.
- This step is to be performed **only** by authorized Imperva personnel.

3. Shut down the appliance and power it off.



Warning: Make sure you are properly grounded before handling the HBA card and the open appliance box.

4. Remove the cover.
5. Locate an empty PCI slot.
6. Insert the HBA card into the empty PCI slot and secure it in place.
7. Close the cover and secure it.
8. Power the appliance on.

Check the HBA Card

9. Log in as `root`.
10. Manually load the Emulex device driver by executing the following command:

    ```
    # modprobe lpfc
    ```
11. Obtain the adapter's WWN by executing the following command:

    ```
    # systool -a -v -c fc_host
    ```

    The following is an example output:

```
Class = "fc_host"
Class Device = "host4"
Class Device path = "/sys/class/fc_host/host4"
active_fc4s = "0x00 0x00 0x01 0x00 0x00 0x00 0x00 0x01
0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 "
fabric_name = "0x20000000c963a4ad"
issue_lip = <store method only>
maxframe_size = "2048 bytes"
node_name = "0x20000000c963a4ad"
port_id = "0x000000"
port_name = "0x10000000c963a4ad"
port_state = "Linkdown"
port_type = "Unknown"
speed = "unknown"
supported_classes = "Class 3"
supported_fc4s = "0x00 0x00 0x01 0x00 0x00 0x00 0x00 0x01
0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 "
supported_speeds = "1 Gbit, 2 Gbit"
symbolic_name = "Emulex LP10000DC-M2 FV1.91A5 DV8.1.10.9"
tgtid_bind_type = "wwpn (World Wide Port Name)"
uevent = <store method only>
Device = "host4"
Device path =
"/sys/devices/pci0000:00/0000:00:06.0/0000:0b:00.2/0000:0d:01.1/host4"
uevent = <store method only>
```

If the driver does not load successfully, there will be no output from the **systool** command.

If the driver does load successfully, a green LED on the adapter will blink until a link is established.

Request that the Storage Manager Add a Logical Volume

12. At this point, ask the local Storage Manager to allocate a Logical Volume on the storage device (using the Storage Manager tools) and configure the partitioning and/or zoning to allow the appliance to access it.

    The information you must provide is:

    - the amount of storage needed, as determined in the first part of this procedure
    - the HBA's WWN, which you obtained in the previous step

      In the example above the number is "**0x10000000c963a4ad**" (see the **port_name** parameter).
    - the type of the operating system, in this case, Linux

    This step may take some time due to maintenance schedules, allocation decisions, *etc.*, so you should perform it as soon as possible.



Note: The zoning should be configured so that the SecureSphere appliance sees only the SCSI target it is supposed to use as a file system.

Physically Connect to the SAN

13. Insert the optical cable connector into the Adapter.

    Pay attention to the Receive/Transmit sides. The other end of the cable should be connected to the appropriate storage device or Fibre Channel switch.

    After a short while the green LED on the adapter should stop blinking. This indicates that a link has been negotiated and established. If this does not happen ask the Storage Manager for help.

Scan the Fibre Channel

At this stage, the driver scans the Fibre Channel for SCSI targets. This operation is performed by the FC device driver, when it is initiated.

14. Unload the driver by executing the following command:

```
# rmmod lpfc
```

15. If you are not using multipath go to step 17.
16. If you are using multipath, then perform the following steps:

    16.1 Open the **`/etc/multipath.conf`** file with a text editor.



Note: The **`/etc/multipath.conf`** file is installed by default when you install the **`device-mapper-multipath`**.

    16.2 Insert a "**#**" character to comment-out the lines that blacklist all devices by default.

    So the following lines:

```
blacklist {
        devnode "*"
}
```

    become:

```
#blacklist {
#        devnode "*"
#}
```

    16.3 Remove the "**#**" character to un-comment the lines that enable the **devnode** blacklist.

    So the following lines:

```
#blacklist {
#       wwid 26353900f02796769
#        devnode "^(ram|raw|loop|fd|md|dm-|sr|scd|st)[0-9]*"
#        devnode "^hd[a-z]"
#}
```

become:

```
blacklist {
        wwid 26353900f02796769
         devnode "^(ram|raw|loop|fd|md|dm-|sr|scd|st)[0-9]*"
         devnode "^hd[a-z]"
}
```

16.4 Perform a dry run and evaluate the setup by by executing the following command:

```
# multipath -v2 -d
```

The output should look like this:

```
mpath1 (3600601602d401e0083e32ef66638de11) dm-4 DGC,RAID 5
[size=100G][features=1 queue_if_no_path][hwhandler=1 emc] \_ round-
       robin 0 [prio=1][active]  \_ 1:0:0:0 sdb 8:16  [active][ready]
       \_ round-robin 0 [prio=0][enabled]  \_ 2:0:0:0 sdd 8:48
       [active][ready]
```

16.5 Start the required multipath processes by executing the following command:

```
# /etc/init.d/multipathd start
```

16.6 Execute the multipath command:

```
# multipath -v2
```

16.7 To get a listing of the current setup, execute the following command:

```
# multipath -ll
```

16.8 Integrate the startup of the appropriate daemons in the boot sequence by executing the following commands:

```
# chkconfig --add multipathd
# chkconfig multipathd on
```



Note: Additional documentation is available in the directory `/usr/share/doc/device-mapper-multipath-x.x.x/`

Update /etc/modprobe.conf

17. Add the following line to the `/etc/modprobe.conf` file:

```
alias scsi_hostadapter lpfc options scsi_mod max_scsi_luns=256
```



Note: If the file already contains `alias scsi_hostadapter`, you must use a different name, for example, `alias scsi_hostadapter1`.

18. Execute the following command:

```
# modprobe lpfc
```

19. Examine the `/proc/partitions` file by executing the following command:

```
# cat /proc/partitions
```

20. Compare the contents of the `/proc/partitions` file with what you recorded in the Make a Note of the Original SCSI Configuration on page 424.

    If your appliance previously had an sda disk and now has an sdb disk as well, then sdb is the disk that has been detected on the Fibre Channel. You will use this information in the following sections, wherever you encounter the sdX notation.



Note: If you are using multipath, the partition is named dm-X, where X is a number.

If you have successfully completed all the steps above, you can proceed to add the newly accessed storage to the Linux operating system.

Create a File System on the SCSI Target

21. Execute the following the command:

    `# mkfs.ext3 /dev/sdX`

    This will create an ext3 file system on the SCSI target at **`/dev/sdX`**.



Note: There is no need to create a partition for the **`/dev/dm-X`** devices. You need only format them using the **`mkfs.ext3 /dev/dm-X`** command, where X is a digit.

Mount the New File System

22. Create a mount point and mount the file system by executing the following command:

    `# mkdir -p /mnt/external-storage`

    `# mount /dev/sdX /mnt/external-storage`



Note: If you are using multipath, the device is named **`/dev/dm-X`** , where X is a digit.

Test the New File System

23. Create a file in the new file system.
24. Remove the file you created in the previous step.

Create a Startup File

You will be creating a startup file that will load the FC module and attach the external storage at boot time, ***before*** SecureSphere starts.

25. Create a startup file named **`/etc/init.d/external-storage`** which consists of the following code:

```
#!/bin/bash
# chkconfig: 35 84 98
# description: Loads the Emulex FC driver
mount_point=/mnt/external-storage
device=/dev/sdX # If you are using multipath, the device is named /dev/dm-X
module=lpfc
prog=$( basename ${0} )
prog=${prog#[SK]??}
function start() {
declare dev=$( basename ${device} )
#
# Probe for LP10000-E or LP11e002. If found, load lpfc.
#
if [ "$(lspci -d 10df:fa00 -n)" ] || [ "$(lspci -d 10df:fe00 -n)" ]; then
modprobe ${module}
if ! grep -qw ${module} /proc/modules; then
echo "${prog}: could not load module \"${module}\""
exit 1
fi
fi
if ! grep -wq ${dev} /proc/partitions; then
echo "${prog}: cannot find \"${dev}\" in /proc/partitions"
exit 1
fi
mkdir -p -m 777 ${mount_point}
mount ${device} ${mount_point}
if ! grep -wq ${mount_point} /proc/mounts; then
echo "${prog}: cannot mount \"${device}\" on \"${mount_point}\""
exit 1
fi
}
function stop() {
umount -f ${mount_point}
rmmod ${module}
}
case "${1}" in
start)
start
;;
stop)
stop
;;
restart)
stop
start
;;
esac
```

26. Link the startup file to the boot/shutdown sequence by executing the following commands:

```
# chmod 755 /etc/init.d/external-storage
# chkconfig --add external-storage
# chkconfig external-storage on
```

Reboot the Machine

27. Reboot the SecureSphere appliance to verify that the required processes automatically start.

    When the machine comes up the new file system should be accessible via the `/mnt/external-storage` mount point.

Configure SecureSphere to Use the SAN

You must configure the SecureSphere appliance to use SAN.

- On a gateway, you can use the SAN to store audit data.
- On a managment server (MX), you can use the SAN to store you can use the SAN to store configuration, event, audit and report archives.
- On a Onebox, you can use the SAN to store both audit data, you can use the SAN to store configuration, event, audit and report archives.

To use the SAN to store audit data:

If you are using the SAN to store the gateway's audit data, configure the SecureSphere gateway or Onebox as follows:

28. Open the `/opt/SecureSphere/etc/bootstrap.xml` file using a text editor.
29. If you are using SecureSphere version 6.2 or higher, change the path of the `audit-base-path` attribute to point to the SAN.
30. If you are using SecureSphere version 6.0.6.X, change the path of the `var-dir` attribute to point to the SAN.
31. Restart the gateway.

To use the SAN to store archive data:

If you are using the SAN to store archive data, configure the SecureSphere MX or Onebox as follows:

32. Start the SecureSphere GUI.
33. In the **Admin** worskpace, click **System Definitions**.
34. In the **System Definitions** pane, select **Action Interfaces**.
35. In the **Interfaces** pane, click .
36. Create a new interface of **Type** NFS Archive.
37. In the **Main** worskpace, click **Policies** > **Action Sets**.
38. Create a new Action Set of type **Archiving**.
39. In the **NFS > Archive** parameter, define the `/mnt/external-storage` mount point.
40. Use the new Action Set as the **Archive Action** (in the **Archiving** tab) in a policy, for example, in an Audit policy.

Disabling the SAN

On the Management Server

Reconfigure archiving actions so that they do not archive to the SAN location.

On the Gateway

To disable SAN on the gateway, you must:

- disable SAN in SecureSphere
- reconfigure the appliance so that it no longer accesses the SAN

To disable SAN on a SecureSphere gateway:

1. Open the **bootstrap.xml** file with a text editor.
2. Restore the **audit-base-path** attribute in the first element to its previous value.

   The default value for Imperva platforms is **/var/SecureSphere**.
3. Restart the gateway.

To reconfigure the appliance so that it no longer accesses the SAN:

1. Login to the appliance as **root**.
2. Execute the following command:un the command:

   ```
   # chkconfig external-storage off
   ```
3. Reboot the appliance.

   You must reboot the appliance in order to cleanly shut down any applications that currently use external storage.

SSL Accelerator

SSL accelerator cards are used to speed SSL processing in SecureSphere appliances. The cards are available for all SecureSphere appliances.

SecureSphere SSL accelerator cards support keys of length 1024 bits and higher.

For more information on SecureSphere SSL accelerator cards, see the Imperva Customer Support Portal (CSP) at www.imperva.com.

LOM (Lights Out Management)

Overview

The LOM (Lights Out Management) add-on is available as a factory installed option for the selected appliances, and enables the following functions to be performed remotely

- power on
- power off
- reboot (reset)

Connecting to the LOM

To connect to the LOM card:

1. Point your browser to https://<IP address of LOM card>



Figure 90 LOM Login window

   The default **IP Address** for LOM card configuration is **http://192.168.0.60**.

2. Enter the **User Name** and the **Password**.

   The default **User Name** is administrator and the default **Password** is password.

3. Click **Login**.

   The **LOM Management** window (Figure 91) is displayed.



Figure 91 LOM Management window

4. Select one of the options by clicking on it.

Managing the LOM

The **LOM Management** window offers the following options:

- General on page 435
- Network on page 436
- Security on page 437

- ANMS (RADIUS Settings) on page 438
- User Management on page 439
- Customization on page 440
- Firmware on page 441
- Power Management on page 442
- Log on page 443
- Logout on page 444

General



Figure 92 General window

The **General** window displays the following parameters:

General Window Parameters

Parameter	Description
Device Name	Enter the LOM card's device name. The name can be up to 16 characters long.
MAC Address	**Read only**: The LOM card's MAC address.
Firmware Version	**Read only**: The version number of the LOM card's firmware.

If the LOM card's IP address is assigned by a DHCP, the address is displayed at the bottom of the window.

Note: Click **Apply** to apply any changes you have made. The changes will not be applied immediately, but only after you logout.

Network

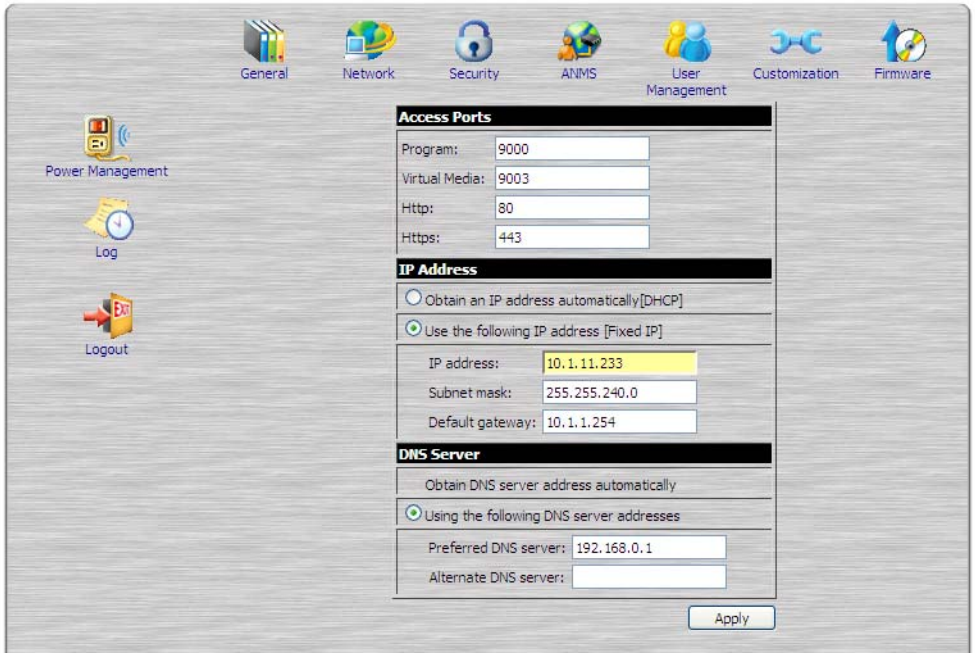


Figure 93 Network window

The **Network** window displays the following parameters:

Network Window Parameters

Parameter	Description
Access Ports	
Programs	The port number used for keyboard, video, mouse and message data transfers. Valid entries are 1024-65536. The default is 9000.
Virtual media	The port number used for data transfer using the virtual media feature. Valid entries are 1024-65536. The default is 9003.
Http	The port number for browser login. Valid entries are 1-65536. The default is 80.
Https	The port number for browser login. Valid entries are 1-65536. The default is 443.
IP Address **Note:** If you change the IP address, then you must check **Reset on Exit** on the **Customization** window (see Customization on page 440) so that the change will take effect.	
Obtain an IP Address Automatically (DHCP)	Obtain a dynamically-assigned IP address using DHCP.
Use the Following IP Address (Fixed IP)	The device has a fixed IP address.
IP Address	Enter the device's fixed IP address.
Subnet Mask	Enter the subnet mask.
Default Gateway	Enter the default gateway.

Network Window Parameters (continued)

Parameter	Description
DNS Server	
Obtain DNS Server address automatically	Select this item to specify that the DNS server's IP address is obtained automatically.
Use the following DNS Server address	Select this item to specify that you will enter the DNS server's IP address in **Preferred DNS Server**. Selecting this option enables the next two items.
Preferred DNS Server	Enter the IP address of the primary DNS server.
Alternate DNS Server	Optionally, enter the IP address of the secondary DNS server.

Note: Click **Apply** to apply any changes you have made. The changes will not be applied immediately, but only after you logout.

Security

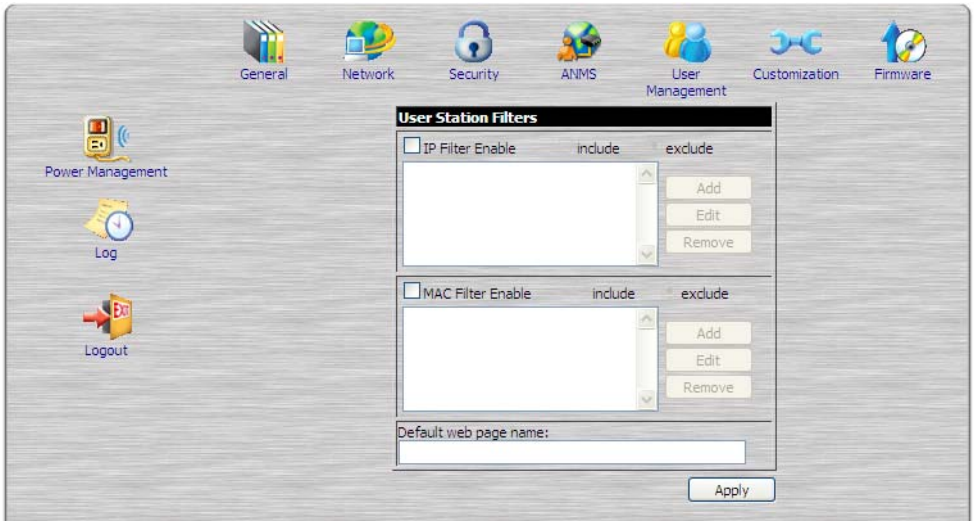


Figure 94 Security window

You can filter access to the LOM card by specifying the IP addresses and/or MAC addresses of devices which are allowed or not allowed to access the LOM card.

To define a filter based on the IP address of the device accessing the LOM card:

1. Select **IP Filter Enable**.
2. Click **Add**.
3. In the first dialog box, enter a starting IP address and click **OK**.
4. In the first dialog box, enter an end IP address and click **OK**.
   Up to 100 IP address ranges can be specified.
5. Select **include** or **exclude** as appropriate.

To define a filter based on the MAC address of the device accessing the LOM card:

1. Select **MAC Filter Enable**.
2. Click **Add**.

3. Enter a MAC address.
4. Select **include** or **exclude** as appropriate.

Defining a Required Login String for Web Browser Access

Default Web page name enables administrators to specify a login string, in addition to the URL, which must be entered when accessing the LOM device using a browser. For example:

192.168.0.2/abcdefg

Users must include the forward slash and the string when accessing the LOM card.

Note: Click **Apply** to apply any changes you have made. The changes will not be applied immediately, but only after you logout.

ANMS (RADIUS Settings)

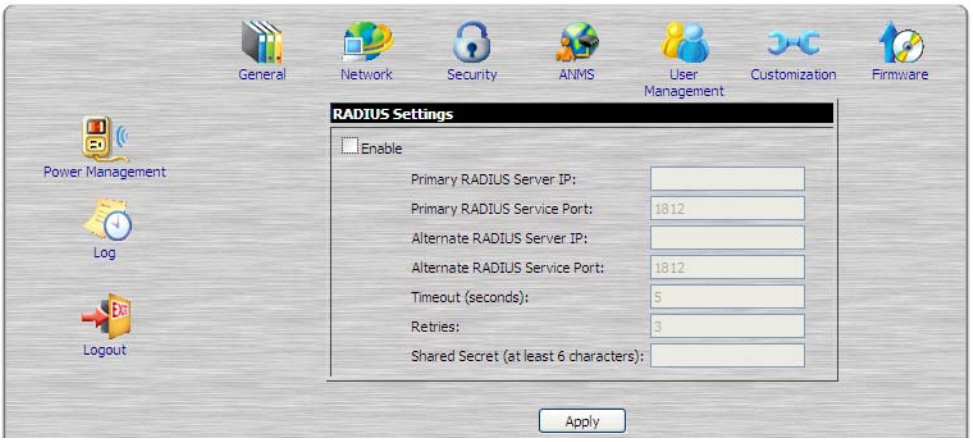


Figure 95 ANMS (RADIUS Settings) window

The **ANMS (RADIUS Settings)** window displays the following parameters:

ANMS (RADIUS Settings) Window Parameters

Parameter	Description
Primary RADIUS Server IP	The IP address of the primary RADIUS server.
Primary RADIUS Server Port	The port number of the RADIUS service on that server.
Secondary RADIUS Server IP	The IP address of the secondary RADIUS server.
Secondary RADIUS Server Port	The port number of the RADIUS service on that server.
Timeout (seconds)	The number of seconds after which a timeout condition is raised while attempting to connect to a RADIUS server.
Retries	The number of times to try to establish the connection to the RADIUS server.
Shared Secret (at least 6 characters)	The shared secret, for authentication with the RADIUS server.

On the RADIUS server, grant users access according to the following table:

RADIUS Permissions

Access Code	Description
C	Grants the user administrator privileges, allowing him or her to configure the LOM card.
W	Allows the user to access the LOM card using the Windows client.
J	Allows the user to access the LOM card using Java.
P	Allows thew user to power on, power off and reset the SecureSphere appliance in which the LOM card is installed.
L	Allows the user to access log information using a browser.
V	Limits to the viewer's access to viewing the video display.

Note:
- The access codes are not case-sensitive.
- A user can be assignee more than one code, separated by commas.
- Click **Apply** to apply any changes you have made. The changes will not be applied immediately, but only after you logout.

User Management

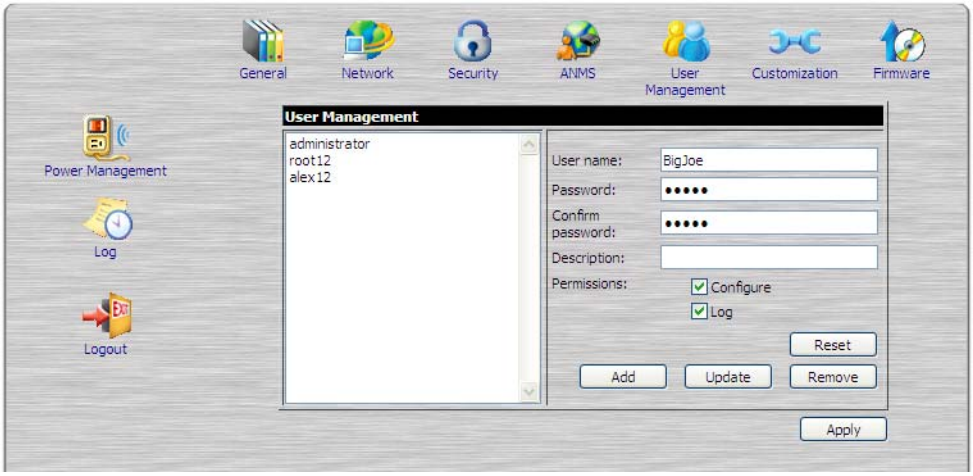


Figure 96 User Management window

The **User Management** window displays the list of users authorized to connect to the LOM card, and enables you to add, edit or delete users.

To add a user:

1. Enter the following parameters for the user:

User Management Window Parameters

Parameter	Description
User name	The user's name (between 6 and 16 characters).
Password	The user's password (between 6 and 16 characters).
Confirm Password	Enter the password a second time, to confirm it.

User Management Window Parameters (continued)

Parameter	Description
Description	**Optional**: information about the user.
Permissions	Define the user's permissions by selecting one or both of **Configure** or **Log**.

2. Click **Add**.

To edit a user:

1. Select the user from the list on the left.
2. Change the user's parameters, as required.
3. Click **Update**.

To delete a user:

1. Select the user from the list on the left.
2. Click **Remove**.



Note: Click **Apply** to apply any changes you have made. The changes will not be applied immediately, but only after you logout.

Customization

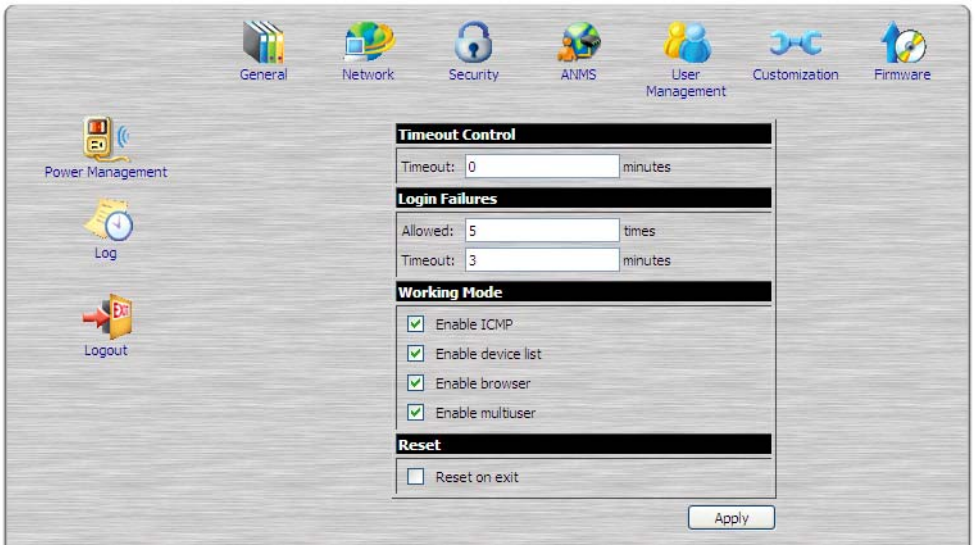


Figure 97 Customization window

The **Customization** window displays the following parameters:

Customization Window Parameters

Parameter	Description
Timeout Control	
Timeout	The session will be ended if there is no input from the connected device for a period of **Timeout** minutes.
Login Failures	
Allowed	The number of failed login attempts a user is allowed, before he is locked out for **Timeout** minutes.
Timeout	The number of minutes a locked out user is prevented from logging in.
Working Mode	
Enable ICMP	If enabled, the LOM card can be PINGed.
Enable Device List	If enabled, the LOM card will be listed among the available devices.
Enable browser	If enabled, the LOM card can be accessed using a browser.
Enable multiuser	If enabled, up to 32 users can access the LOM card simultaneously.
Reset	
Reset on exit	Reset the LOM card when exiting this application.

Note: Click **Apply** to apply any changes you have made. The changes will not be applied immediately, but only after you logout.

Firmware

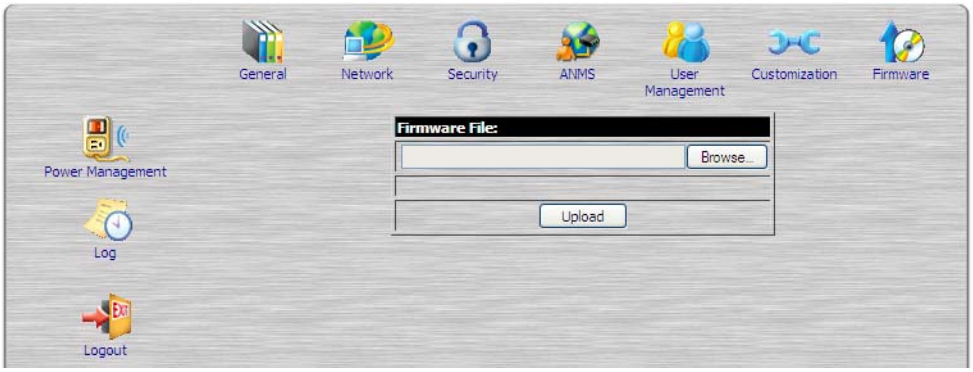


Figure 98 Firmware window

The **Firmware** window enables you to upgrade the LOM card's firmware from a file you have previously downloaded.

To upgrade the firmware:

1. Browse to the file containing the firmware.
2. Click **Upload**.

Note: The firmware will be updated after you restart the appliance.

Power Management

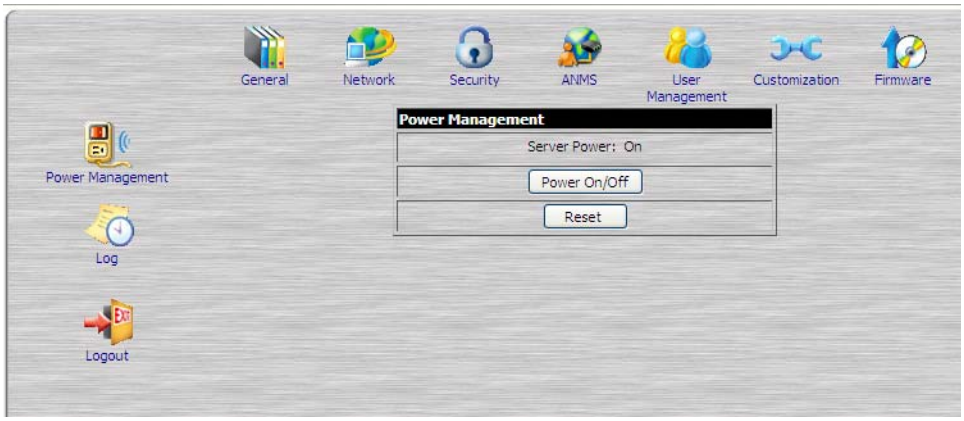


Figure 99 Power Management window

The **Power Management** window displays the following parameters:

Power Management Window Parameters

Parameter	Description
Server Power	Indicates whether the SecureSphere appliance is on or off.
Power On/Off	Click to power the SecureSphere appliance on or off, as appropriate.
Reset	Click to reset the SecureSphere appliance.

Note: Click **Apply** to apply any changes you have made. The changes will not be applied immediately, but only after you logout.

Log

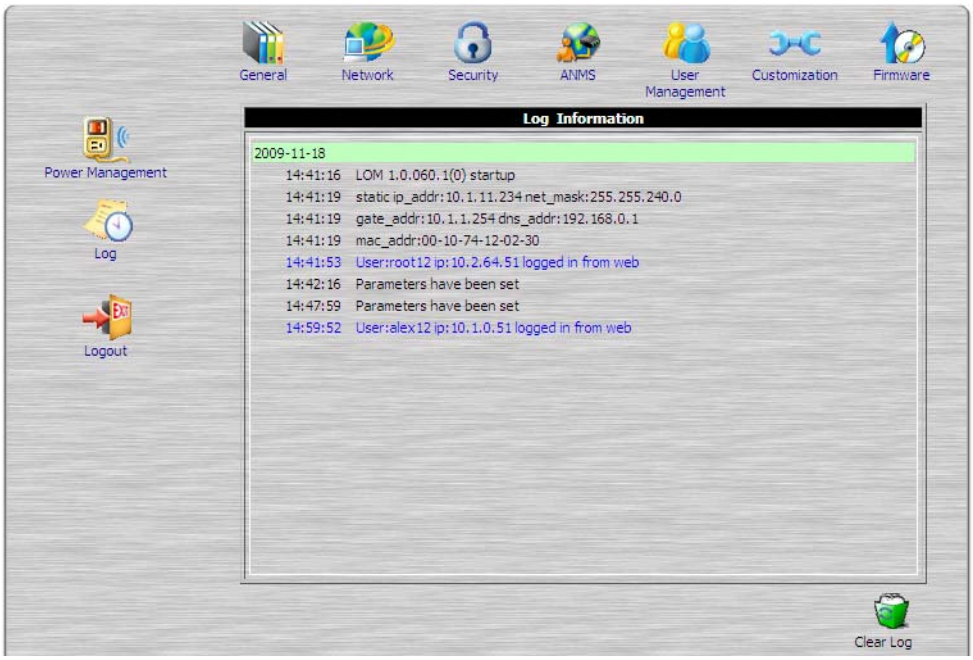


Figure 100 Log window

The **Log** window displays the events log.

To clear the events log, click the **Clear Log** icon.

Logout

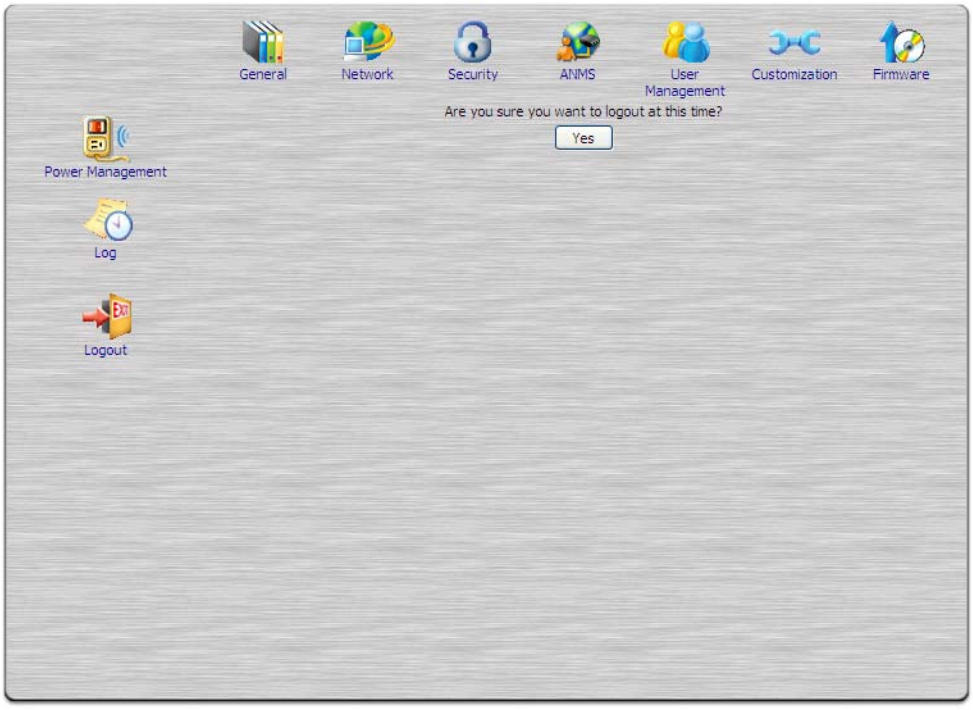


Figure 101 Logout window

If there are pending changes that have not yet been applied, a message will be displayed to that effect. The changes will be applied after you logout.

To logout, click **Yes**.

APPENDIX E

Command Line Interface

This chapter is a reference to the SecureSphere command line tools:

- impcfg on page 446
- impctl on page 452
- Miscellaneous Commands on page 455

impcfg

impcfg Functionality Map

Table shows the complete **impcfg** functionality.



Note: (I) means immediate activation, that is, the command is executed and, if relevant, the SecureSphere database is updated immediately.

impcfg Functionality Map

Top Screen Menu	Level 1 menu	Level 2 menu	Level 3 menu	For more information, see
Manage SecureSphere Server	Deactivate server			Configuring a Management Server on page 69
	Restart server **(I)**			
	Stop server **(I)**			
	Change management password			
	Change database password			
	Deactivate server			
Manage SecureSphere Gateway	Perform actions (start, stop, etc.)	Unregister gateway **(I)**		Configuring a Gateway on page 71
		Soft gateway restart **(I)**		
		Hard gateway restart (teardown/ prepare resources) **(I)**		
		Stop gateway **(I)**		
		Refresh gateway status **(I)**		
Manage SecureSphere Gateway *(continued)*	Change gateway name			
	Change server address /password			

impcfg Functionality Map (continued)

Top Screen Menu	Level 1 menu	Level 2 menu	Level 3 menu	For more information, see
	Change operation mode	Sniffing		Configuring a Gateway as a Sniffing Gateway on page 75 **Note:** The management server must be running when you execute this command.
		Bridge STP		Configuring a Gateway as a Bridge on page 73
		Bridge IMPVHA		
		Reverse Proxy Apache		Configuring Apache Reverse Proxy on page 110
		Reverse Proxy Kernel		Configuring Kernel Reverse Proxy on page 103
	Manage hardware security modules (HSM)	enable nCipher HSM		Hardware Security Modules (HSM) on page 400
		enable SafeNet HSM		
	Manage remote agents	Add a legacy (pre 7.0) agent		Managing Remote Agents on page 76
		Modify a legacy (pre 7.0) agent		
		Delete a legacy (pre 7.0) agent		
		Add agent listener		
		Delete agent listener		
		Add z/OS agent listener(s)		
		Delete z/OS agent listener		
		Manage remote agent routes		

impcfg Functionality Map (continued)

Top Screen Menu	Level 1 menu	Level 2 menu	Level 3 menu	For more information, see
Manage SecureSphere Gateway *(continued)*	Manage interfaces and routes *(for a bridge)*	Create bridge		Configuring a Gateway as a Bridge on page 73
		Delete bridge		
		Toggle STP on a bridge		
		Toggle High Availability on a Bridge		
	Manage interfaces and routes *(for a sniffing gateway)*	Set sniffing interface(s)		Configuring a Gateway as a Sniffing Gateway on page 75
		Set blocking interface		
		Add/modify blocking mask		
		Delete blocking mask		
	Manage interfaces and routes *(for a Kernel Reverse Proxy)*	Add alias		Configuring Kernel Reverse Proxy on page 103
		Modify Alias		
		Delete Alias		
		Enable high availability		
		Manage reverse proxy (kernel) routes		
	Manage interfaces and routes *(for an Apache Reverse Proxy)*	Add alias		Configuring Apache Reverse Proxy on page 110
		Modify Alias		
		Delete Alias		
		Enable high availability		
		Manage reverse proxy (kernel) routes		

impcfg Functionality Map (continued)

Top Screen Menu	Level 1 menu	Level 2 menu	Level 3 menu	For more information, see
Manage SecureSphere DAS	Deactivate server			Configuring a Data Assessment Server (DAS) on page 81
	Restart server **(I)**			
	Stop server **(I)**			
	Change management password			
	Change database password			
	Deactivate server			

impcfg Functionality Map (continued)

Top Screen Menu	Level 1 menu	Level 2 menu	Level 3 menu	For more information, see
Manage platform	Manage network	Management interface	Change device	Management Interface on page 86
			Change IP address	
			Change netmask	
			Locate device **(I)**	
		LAN interface	Change device	LAN Interface on page 88
			Change IP address	
			Change netmask	
			Locate device **(I)**	
		Default gateway		Default Gateway on page 89
		Static routes	Add route	Static Routes on page 89
			Delete route	
		Name Resolution (DNS client)	Enable DNS client	Name Resolution (DNS client) on page 90
			Set domain	
			Set search list	
			Set name servers	
		Locate network devices		Locate Network Devices on page 91
	Manage time	Add time server		Time Servers on page 92
		Delete time server		
	Manage users			Users Management on page 92
	Manage hostname			Hostname Management on page 97
	Manage bootloader password			Bootloader Password Management on page 98
	Reboot the appliance **(I)**			Configuring the Platform on page 84
	Shutdown the appliance **(I)**			Configuring the Platform on page 84

impcfg Functionality Map (continued)

Top Screen Menu	Level 1 menu	Level 2 menu	Level 3 menu	For more information, see
Upgrade / updates				This option is reserved for future use.

impctl

impctl is a lower level configuration tool that runs on the appliances. **impcfg** runs **impctl** on the appliance to deploy the configuration that the administrator defines in **impcfg**.



Warning: **impctl** is for highly experienced administrators only. Inexperienced users can seriously damage the appliance's configuration, requiring reinstallation from scratch, and they should therefore use **impcfg** instead

"Safe" impctl Commands

The table below lists the commonly used "safe" **impctl** commands.

impctl - Selected "Safe" Functionality

impctl command	Description
`impctl show commands --verbose`	List **impctl** commands and their arguments.
`impctl status`	Display the status of the appliance.
`impctl server start`	Start the MX server.
`impctl server stop`	Stop the MX server.
`impctl server restart`	Stop and then start the MX server.
`impctl server ha password --set-database-password=NEW_SYSTEM_PASS --set-server-password=NEW_SECURE_PASS`	Change system (database) and/or secure (system) password on HA-MX server. For more information about SecureSphere users and passwords, see The Different SecureSphere Users on page 56.
`impctl gateway start`	Start the gateway.
`impctl gateway stop`	Stop the gateway.
`impctl gateway restart`	Stop and then start the gateway.
`impctl gateway register`	Register the gateway to its MX server.
`impctl gateway unregister`	Unregister the gateway from its MX server.
`impctl gateway config --encryption=yes`	Encrypt database audit files stored on the gateway.
`impctl hardening config --root-source-ip-exception=<IP address>`	Specify an IP address from which user root is allowed to login over SSH.

Stopping and Starting the MX in an MX-HA Environment

The correct way start and stop the MX in an MX-HA environment is by using the following commands:

```
impctl server ha start
impctl server ha stop
```



Warning: Do not use **impcfg** or **impctl** to start and stop the MX as you would in a non-MX-HA environment (as described in Configuring a Management Server on page 69). Use only the above commands.

Miscellaneous impctl Commands

Disk Maintenance

Use the following command on MX appliances with mirrored disks to determine if a disk has failed.

impctl platform storage raid adaptec arcconf getconfig 1

The status of the appliance's disk drives is displayed.

Below is an example of a portion of the command's output. Note that in this example, "Device 0" has failed (its State is given as "Failed").

```
---------------------------------------------------------------------
Physical Device information
---------------------------------------------------------------------
      Device #0
         Device is a Hard drive
         State                              : Failed
         Supported                          : Yes
         Transfer Speed                     : Failed
         Reported Channel,Device            : 0,0
         Reported Location                  : Connector 0, Device 0
         Vendor                             : WDC
         Model                              : WD1002FBYS-02A6B
         Firmware                           : 03.00C06
         Serial number                      : WD-WMATV1847734
         Size                               : 0 MB
         Write Cache                        : Unknown
         FRU                                : None
         S.M.A.R.T.                         : No
      Device #1
         Device is a Hard drive
         State                              : Online
         Supported                          : Yes
         Transfer Speed                     : SATA 3.0 Gb/s
         Reported Channel,Device            : 0,1
         Reported Location                  : Connector 0, Device 1
         Vendor                             : WDC
         Model                              : WD1002FBYS-02A6B
         Firmware                           : 03.00C06
         Serial number                      : WD-WMATV1847454
         Size                               : 953869 MB
         Write Cache                        : Enabled (write-back)
         FRU                                : None
         S.M.A.R.T.                         : No
```

To determine which disk is “Device 1”, use the following command:

```
impctl platform storage raid adaptec arcconf IDENTIFY 1 DEVICE 0 1
```

To determine which disk is “Device 0”, use the following command:

```
impctl platform storage raid adaptec arcconf IDENTIFY 1 DEVICE 0 0
```

If this command is successful, the LED of the device lights up. If the device has failed, the command may not succeed, that is, the LED may not light up, depending on the nature of the failure.

Miscellaneous Commands

Powering Down the Appliance

Note: This section relates only to the NG (X series and M series) appliances.

Both of the following OS commands power down the appliance:

- `poweroff`
- `shutdown -P now`

After using either of these commands to power down the appliance, you must remove the power cord and re-insert it before powering up the appliance again.

For appliances with only one power supply, you can alternatively wait two minutes before powering up the appliance again.

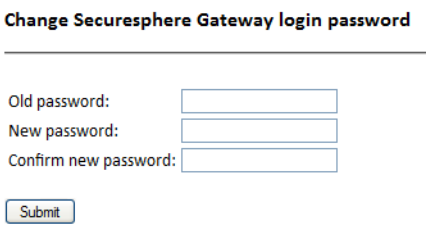
Warning: These commands are the only correct, supported ways to power down the appliance.

Changing the Password for Management Server - Gateway Communication

Communication between a management server and its gateways (including gateway registration to the management server) is secured by a password. The default password is “secure”.

To change the Password for Management Server - Gateway Communication:

1. Open a browser and go to the gateway’s port 443 using HTTPS, for example:
   `https://10.1.1.10:443/`
2. Enter the user “`imperva`” and the current password.
   The default password is “`secure`”.
3. From the menu, click **Change the Gateway’s login password**.
4. In the **Change SecureSphere Gateway login password** screen, enter the following information:
   - **Old password**
   - **New password**
   - **Confirm new password**



5. Click **Submit**.

APPENDIX F

FIPS 140 Compliance

This chapter describes on SecureSphere FIPS (Federal Information Processing Standard) 140-2 compliance, and includes:

- Compliance on page 458
- Activating FIPS Mode on page 461

Compliance

2.1 Encrypted Communications

SecureSphere uses FIPS-certified encryption modules to perform cryptographic operations within the cryptographic boundary. The cryptographic modules used by SecureSphere are compiled and operated in FIPS mode and perform the appropriate self tests at initialization.

2.2 MX Encrypted Communications

SecureSphere's Management Server operates under Java JRE version 1.6. As part of its operation it performs cryptographic operations such as archiving, communications to clients, and communications with the gateways it manages. All of these operations are performed by the RSA Crypto-J version 4.0 FIPS package which is certified at FIPS level 1.

The NIST certificate number is 1048 (see http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2008.htm#1048).

2.2.1 FIPS-Approved Algorithms

The following algorithms are applied when using Crypto-J in FIPS mode:

- AES (Cert. #669)
- DSA (Cert. #251)
- ECDSA (Cert. #72)
- HMAC (Cert. #353);
- RNG (Cert. #389 and vendor affirmed: SP 800-90)
- RSA (Cert. #311)
- SHS (Cert. #702)
- Triple-DES (Cert. #614)

2.2.2 FIPS-Non-Approved Algorithms

The following algorithms are **not** approved when using Crypto-J in FIPS mode:

- AES-GCM (non-compliant)
- DES
- Diffie-Hellman
- DESX
- ECAES
- EC Diffie-Hellman
- ECIES
- RNG (X9.31 non-compliant, MD5 and SHA1)
- RC5
- RSA OAEP (for key transport)
- RSA Keypair Generation MultiPrime
- RSA (key wrapping; key establishment methodology provides between 80 and 150 bits of encryption strength; non-compliant less than 80 bits of encryption strength);
- HMAC-MD5
- Raw RSA
- RC4
- RC2

- ECDHC
- MD2
- MD5
- PBE (SHA1 and Triple-DES)
- RIPEMD 160

2.3 SecureSphere Gateway and Platform Communications

SecureSphere Gateway and platform communications are accomplished using OpenSSL version FIPS 1.1.2. This OpenSSL version is used for all incoming and outgoing connections related to the SecureSphere daemon.

OpenSSL FIPS 1.1.2 is FIPS-certified with overall level 1 with certificate number 918 (see http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140crt/140crt918.pdf).

2.3.1 FIPS-Approved Algorithms

The following algorithms are applied when using OpenSSL in FIPS mode:

- Triple-DES (Cert. #613)
- AES (Cert. #668)
- SHS (Cert. #701)
- HMAC (Cert. #352)
- RSA (Cert. #310)
- RNG (Cert. #387)

2.3.2 FIPS-Non-Approved Algorithms

The following algorithms are **not** approved when using OpenSSL in FIPS mode:

- DES
- Diffie-Hellman (key agreement; key establishment methodology provides between 80 and 256 bits of encryption strength);
- RSA (key wrapping; key establishment methodology provides between 80 and 150 bits of encryption strength);
- DSA (Cert. #250; non-compliant)

2.4 HSM solution

SecureSphere can be integrated with nCipher's netHSM which is FIPS level 2 (or 3, depending on configuration) certified, which provides FIPS-certified key storage solutions. For more information, see Imperva's support site for solution number 903.

2.5 SecureSphere WAF in FIPS Mode

In order to decrypt web traffic in FIPS mode, SecureSphere uses the FIPS-certified NSS cryptographic module. The module is both level 1 and 2 certified. SecureSphere uses it in level 1 with NIST certificate #815 (see http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2007.htm#815).

In order to decrypt in FIPS mode you need to configure the server group address to be the internal address of the web server and decrypt the traffic using SecureSphere reverse proxy Apache mode, while keeping the server side traffic clear (or vice versa).

Limitations

The following features are **not** supported in FIPS mode:

- Assessment – all tests that are categorized as “OS Level”
- Assessment – all tests that are categorized as “Track Changes”
- Action Sets – Archive to SCP Location Action Interface
- Web KRP (Kernel Reverse Proxy) when the KRP encrypts/decrypts data
- Web TRP (Transparent Kernel Reverse Proxy) when the TRP encrypts/decrypts data
- RSA keys shorter than 1024 bits

Activating FIPS Mode

To activate FIPS mode:

1. In the **Admin** workspace, click **System Definitions**.
2. In the **System Definitions** pane, select **FIPS Settings**.
3. Enable **FIPS Mode**.
4. Click **Save**.

   If you are in delayed activation mode, you need to activate this settings. For further information, see the **SecureSphere User Guide**.

APPENDIX G

Disaster Recovery

This appendix details disaster recovery procedures for the SecureSphere management server.



Note: The features described in this appendix are available in SecureSphere versions 7.5 Patch 6 and later.

Disaster Recovery

In the event that a management server becomes unusable, it is possible to transfer its data to another machine on which the SecureSphere management server has been installed.

For information on exporting and importing management server data, see Exporting and Importing the Management Server on page 262.

Preparing for Disaster Recovery

To prepare for disaster recovery:

1. Prepare a standby server in another location.
2. On the active management server, install two licenses, one for the active server and one for the standby server.

   For information on installing licenses, see Chapter 8, Licenses.
3. Whenever you upgrade the active management server to a new version of SecureSphere, upgrade the standby server to the same version.
4. On a scheduled basis, export the management server data and store the exported data off-site.



Note: The exported data include SSL keys and licenses.

Recovery

To configure the standby management server:

1. Confirm that the standby management server is running the same version of SecureSphere (including patches) that was running on the primary management server.
2. Import the exported data to the standby management server.
3. Re-register the SecureSphere gateways to the standby management server (see Configuring a Gateway on page 71) by running the script in the next section (Automatically Re-registering the Gateways on page 464).



Note: The secondary management server must be up and running when you perform this step.

Automatically Re-registering the Gateways

You can simplify the gateway registration process by automatically re-registering the gateways to the management server.

To automatically re-register the gateways:

1. On the management server, execute the following command:

```
impctl force-remote-registration --mx-ip=10.1.5.117 --mx-password='secure12'
[--gateway-password='different_password']
```

force-remote-registration Parameters

Parameter	Description
`--mx-ip`	The IP address of the standby management server.
`--mx-password`	The secure user password for the gateway. For more information, see SecureSphere Users on page 56.
`--gateway-password`	**Optional** : The password for gateway-MX SSL. If this parameter is not specified, then the default password is used. If the password is not the same for all gateways or is not correct, you will prompted for each password.

The first two parameters are required.

Error messages are output to the management server's `impctl` log and to `stderr`.

If one gateway cannot be registered, the script will continue to try to register the other gateways.

You can also see the registration in the gateway's log by executing the following command on the gateway:

```
impctl show log --verbose
```

The `--verbose` parameter adds the date and time to each output line.

APPENDIX H

PCI Compliance

This appendix describes PCI compliance, and includes:

PCI Data Security Standard on page 466
PCI Compliance on page 467

PCI Data Security Standard

PCI DSS requirements apply to all system components that are included in or connected to the cardholder data environment. The cardholder data environment is that part of the network that possesses cardholder data or sensitive authentication data, including network components, servers and applications.

- Network components may include but are not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances.
- Server types may include but are not limited to the following: web, database, authentication, mail, proxy, network time protocol (NTP), and domain name server (DNS).
- Applications may include but not limited to all purchased and custom applications, including internal and external (Internet) applications.

SecureSphere and PCI DSS

SecureSphere can assist administrators in achieving PCI compliance for their systems by tracking, monitoring and, if necessary, blocking access to cardholder data. At the same time, SecureSphere management servers, gateways and remote agents are considered network components in the cardholder data environment, and are thus themselves subject to the PCI DSS.

The requirements relevant to SecureSphere fall into the following areas:

- Protecting the SecureSphere appliance itself, for example, through the use of firewalls. For more information, see Protecting the SecureSphere Appliance on page 467.
- Protecting cardholder data stored by SecureSphere or in transit between protected systems and the SecureSphere appliance. For more information, see Protecting Cardholder Data on page 467.

PCI Compliance

Protecting the SecureSphere Appliance

The default SecureSphere configuration provides protection for the SecureSphere appliance as follows:

1. Root and secure user access (see SecureSphere Users on page 56) to the appliance OS is available only locally, and not over SSH. SSH access to the appliance OS is available only for users other than **`root`** and **`secure`** (see CLI Users on page 57), and these users can execute only a limited set of OS commands.
2. Passwords for all SecureSphere administrators and users must be at least 7 characters long, and contain at least 1 alphabetic and at least 1 numeric character, in conformance with PCI requirements.
3. The default SecureSphere administrator is required to change his password the first time he logs in to SecureSphere.
4. All SecureSphere administrators and users must change their passwords at least every 90 days. The new password cannot be the same as one of the previous four passwords.
5. All SecureSphere administrators and users are locked out after six consecutive failed authentication attempts.
6. GUI and CLI sessions are terminated automatically after 15 minutes of inactivity.
7. SecureSphere log files are accessible only by authorized administrators.
8. SecureSphere logs all administrator access (logins) to SecureSphere appliances and to the SecureSphere GUI.
9. SecureSphere uses SSH to secure administrative access to the SecureSphere management server, and SSL/TLS to secure connections between the SecureSphere management server and SecureSphere gateways.

In addition, administrators should restrict the physical access to the SecureSphere appliance to authorized personnel only.

Protecting Cardholder Data

To protect cardholder data, the SecureSphere administrator should configure SecureSphere as follows:

1. Configure the SecureSphere gateway to mask cardholder data before storing audit data locally. The audit data transmitted to the SecureSphere management server to be stored there will then be in masked form.

   For information on masking sensitive data, see the “Configuring Data Masking Options” section in Chapter 2 of ***SecureSphere User Guide***.
2. Encrypt audit data stored on the SecureSphere gateway, which remain encrypted when transmitted from the gateway to the management server and stored there.

   For information on how to configure this option, see the “Configuring Encryption” section in the Maintenance chapter of the ***SecureSphere Administration Guide***.
3. Encrypt audit archives. For information on encrypting archives, see the “Managing Archive and Key Settings” section in the “Advanced SecureSphere Configuration” chapter of the ***SecureSphere User Guide***.
4. Encrypt the data channel between the SecureSphere gateway and the SecureSphere Remote Agents installed on the database server, so that data transmitted over this channel (which will be masked only on the gateway) are not exposed.

   In **`impcfg`**, configure the Remote Agent data channel to use SSL. For more information, see the “Managing Remote Agents” section in the “Configuring SecureSphere” chapter of the ***SecureSphere Administration Guide***.

Symbols

/etc/hosts file
duplicate names **355**

/var/log/secure **56**, **57**

$ORACLE_HOME **165**

Numerics

10G appliances **217**

A

accountability **56**

action interface
NFS archive **214**

action interface type
action set event type correlation **302**

Action Set **263**

action set event type
action interface type correlation **302**

action URLs
maximum per application **291**

Active Directory
Global Catalog **315**

ADC
manual updates **249**
scheduled updates **249**
using a proxy **306**

ADC database
exporting during update **264**, **266**

admin CLI command **57**

admin user
LDAP authentication **313**

Admin workspace
access to **232**

AIX
post installation **137**
restarting DB2 database instances after installing Remote Agent **137**

Apache
encryption **112**

Apache Reverse Proxy
configuring **110**

configuring with Kernel Reverse Proxy **117**
RSA Clear Trust **112**

appliances
powering down **455**

archiving
directly from gateway **214**
per gateway **214**

Archiving action **263**

AS400 **319**

ASCII **306**

assessment tests
legacy **305**

audit **292**, **293**

audit archive directory
mounting **214**

audit archiving
direct **212**

audit data
encrypting **328**

audit directory
changing the path **327**

audit directory path
changing **327**

audit enrichment
URM **306**

audit files
encryption **452**

authentication
external **97**

B

background process **331**, **334**

Backspace key **43**, **46**, **61**

Basel II report **318**

bash **122**

BEQ **165**

bootloader **98**

bootstrap.xml
NATed gateways **163**

bottlenecks
identifying **335**

buffering **150**

built-in stored procedures
definition **323**

bypass mode **75**

C

CA Detector for DB2 for z/OS **189**, **208**

CHAP **97**

checksum

IP **217**
TCP **217**
UDP **217**

CIDR
specifying for MX **71**

Cisco
PVST PDU **74**

CLI users **56**

COLLID pamater **189**, **208**

command line
changing passwords from **69**

command line scripting **168**

comments
Security Policy **321**

configuration wizard
Remote Agent **137**

Connected Users **245**

console
access to SecureSphere **388**

cookies
maximum per application **291**

counters **149**

CPU affinity **26**

CPU load **330**

CSV file **331**, **334**

CSV files
uploading **305**

D

DAC **167**

DAS
reconfigure as Onebox **83**

data interfaces
automatic discovery **136**
manual configuration **136**, **165**

Data Owner **306**

database
recreating **364**

database password
changing **69**

database user groups
maximum per application **290**

database users
maximum per application **290**

databases
maximum per user **288**

DB Agents
moving a gatewat to another group **212**

DB2
after installing the Remote Agent on AIX **137**

decision rules

Kernel Reverse Proxy **106**, **108**

deployment modes
switching **118**

df **123**, **128**

DHCP
IPv6 **54**

direct archiving **214**

direct audit archiving **212**

disaster recovery
preparing for **463**
recovering **463**

disk
failed **453**

DNS **386**
IPv6 **53**

DNS client **313**

DNS servers **90**

driver
Remote Agents **141**

drop-in replacement **30**

E

EBS report **318**

Emulex **422**

encryption **112**, **126**, **150**
audit data **328**
audit files **452**
Default Archive Settings **258**, **260**, **269**, **272**

error page
sniffing mode **37**

events
definition of **334**

export
SecureSphere configuration **262**

exporting
to a non-default directory **263**

external authentication **97**

external systems
IPv6 **55**

F

Fail Close **216**, **217**

Fail Open **217**

failed disk **453**

fake key
nCipher **406**

FAM **306**

Fast Viewing
number of days to retrieve **256**

FIPS 140-2 **299**

FIPS compliant mode **411**

firewall
- between Remote Agent and listener **126**, **163**

first-time configuration
- running a second time **59**
- sequence **59**

First-Time Login **59**

forward compatibility **40**

full_expimp **264**
- while ADC is being updated **264**, **266**

G

gateway
- converting to Onebox **118**
- initial configuration **59**
- register to MX **71**
- registering and unregistering **59**
- start **71**
- stop **71**
- unregister **71**

gateway groups
- Fail Close **216**
- Fail Open **216**
- High Availability **216**
- mode **215**

gateway IP address **127**

gateway physical interface **127**

gateway registration
- password **455**

gateway registration failure **140**

Gateways
- maximum server groups **38**

gateways
- archiving directly from **214**
- automatically re-registering **464**
- moving to another group and DB Agents **212**, **213**
- refresh status **72**
- register, unregister **72**
- restart **72**
- stop **72**

GLBA report **318**

Global Catalog **315**

GRUB
- see bootloader **98**

GUI
- language **325**

H

Hardware Security Module
- see HSM **400**

High Availability **34**, **127**, **150**
- and STP **74**
- configure on a bridge **74**
- network **372**

HIPAA report **318**

host names
maximum per user **288**

hostname **322**
"
" character **53**
"-" character **355**
changing **97**

hostname resolution
forward and reverse **124**

hosts
maximum per application **289**

HSM **400**

HTTP Archive
Action Interface type **302**

httpd.conf **117**

HTTPS Archive
Action Interface type **302**

hypervisor
Remote Agents **154**

hyphens
in hostname **355**

I

impcfg **57**, **313**
MX-HA **60**, **350**
when changes are applied **63**

impctl
commands **452**
MX-HA **60**, **350**

import
SecureSphere configuration **262**

IMPVHA **102**, **341**

IMPVHA Bridge **215**

Initial Sequence Number
see ISN **217**

interface
external **125**
gateway physical **151**
loopback **125**

inter-process communications **125**

IP address
active MX-HA server **330**

IP checksum **217**

IPC **125**, **165**

ipc.dll **137**

IPv6
address formats **52**
CIDR **53**
default gateway **54**
DHCP **54**
dual stack **53**
external systems **55**

gateway syslog **53**
LDAP **313**
link-local addresses **54**
lookup datasets **52**
MX syslog **53**
MX-Gateway communication **53**
MX-Gateway communications **53**
MX-HA **54**
Remote Agents **54**
SecureSphere Agent for DB2 z/OS **54**
SecureSphere GUI **53**
static routes **89**
support for **52**
ThreatRadar **52**
VRRP **54**

IPv6 addresses
equivalence of different forms **52**
treated as character strings **52**

IRQ affinity **26**

ISN **217**

ISO 27001 report **318**

J

job
displaying schedule **253**

jobs
aborting **254**
displaying status of **253**
followed action **254**
scheduling **254**

Jobs Status window **253**

K

kernel
upgrading SUSE kernel **130**

Kernel Reverse Proxy **32**, **215**
configuring **103**
configuring with Apache Reverse Proxy **117**

keys
RSA **460**

KRP **32**
FIPS 140 compliance **460**
VRRP **106**

L

language
GUI display **325**

LDAP **86**, **90**, **306**, **313**
case sensitivity **237**
IPv6 **313**

legacy assessment tests **305**

legacy deployments **30**

licenses
MX-HA **222**

Lights Out Management **434**

link-local addresses **54**

Linux
top command **330**, **335**

listener IP address **126**

listeners
multiple **78**, **125**

Load Balancer **34**

locking a user **95**

log file
wizard errors **138**

login URLs
maximum per application **291**

logs **153**

LOM **434**

lookup **320**

lookup data **320**

lookup datasets
IPv6 **52**

loopback
MySQL **167**

loopback interface **125**

LSO **161**

Luna
importkey command **420**

LunaSA **400**, **411**
SecureSphere integration **411**

M

MAC addresses **154**
re-registering Remote Agent after change to **154**

machine load **330**

management password
changing **69**

management server
initial configuration **59**
performance data **330**

management server-gateway communication
changing password **455**

Management Servers
maximum server groups **38**
maximum SSL certificates **38**

MS-CHAP **97**

multiple Oracle instances **165**

MX
see management server

MX-HA
confirming configuration **365**
hardware requirements **353**
impcfg and impctl **60**, **350**
IP address of active server **330**

IPv6 **54**
licenses **222**
software requirements **353**
starting and stopping **60**, **453**

MySQL
directing traffic over loopback **167**
driver **49**

N

NAT **126**, **163**
bootstrap.xml file **163**

nCipher **406**

nCipher card **400**

nCipher netHSM **400**

netHSM **406**

network interface
physically locating **87**, **88**, **91**

Network Trust Link
see NTL **413**

NFS
archiving **214**

NFS Archive
Action Interface type **302**

non-Transparent Reverse Proxy
description **32**

nss.conf **117**

NTL **413**

NTP **91**, **386**
IPv6 **53**

NTP servers
adding and deleting **92**

O

OEL UEK **122**
Remote Agents **130**

Onebox
converting to gateway **118**
forward compatibility **40**

OS
hardened **57**

P

PAP **97**

parameters
maximum per application **290**
maximum per URL **289**

passwd **57**

password **148**
different from previous **299**
expiration **299**
gateway-management server communication **455**
lower-case characters **299**
minimum length **299**

non alpha-numeric characters **299**
numeric characters **299**
upper-case characters **299**
valid characters **360**

passwords
changing **57**, **364**
expiration **57**
length **57**
maximum length **57**
minimum length **57**
strength **57**
valid characters **57**

patches
OS and database **121**

patching MX-HA **353**

PCI report **318**

PeopleSoft report **318**

performance profiling **218**, **333**

ping **54**

ping6 **54**

plugin **288**

port 443 **148**

port configuration
conflict **102**

portguard
IPv6 **54**

ports
443 **125**
registration **148**

Posix **91**

POST **33**
maximum length **33**
multi-parts **33**

power cord
removing and reinserting **455**

power source **41**

powering down **455**

powering down the appliance **455**

poweroff command **455**

pre-install script
Remote Agents **123**

prepare **99**

Privacy report **318**

private keys
secure storage **400**

profile
size limits **288**

profile size violation **288**

PVST PDU **74**

PXE client **391**

Q

queries
larger than 4K **296**
maximum per application **289**
maximum per query group **291**
query groups
maximum per user **291**

R

RADIUS **96**, **97**, **315**, **438**
supported authentication schemes **97**
ragent process **155**
register
gateway to MX **71**
registration **139**, **148**
Remote Agent listeners
defining on same port with SecureSphere Agent for DB2 z/OS listener **77**, **78**, **79**, **125**, **174**
Remote Agents **303**
communications protocol **134**
configuration wizard **128**, **131**, **137**
define traffic to monitor **138**
downgrading **137**
external interfaces **125**
gateway IP address **134**
High Availability **140**, **150**
hypervisor **154**
IPv6 **54**
latest version **121**
Management Console log file **153**
management listener port **135**
maximum per gateway **38**
monitor local trafic **135**
moving a gateway to another group **213**
name **134**
non-Windows silent install **128**
pre-7.0 versions **121**
primary gateway **140**
registration **125**
registration failure **140**
Release Notes **122**
removing the driver **141**
re-registering after MAC address change **154**
secondary gateway **140**
SharePoint **124**
silent uninstall **142**
special considerations for SUSE **130**
uninstall **141**, **142**
unregister **154**
upgrading **137**
VMware **154**
Windows silent install **131**
Reverse Proxy Apache **215**
risk score
update schedule **270**
RSA
FIPS 140 compliance **460**

RSA Clear Trust **117**

S

SafeNet LunaSA **400**

SAN **422**
- configuring **423**
- disabling **431**
- X-series appliances **425**

SAP report **318**

SAP transactions
- defining **396**
- monitoring **395**

scanning
- SSH Proxy **316**

scheduling
- jobs **254**

SCP **57**
- archiving **214**
- FIPS 140 compliance **460**

SecureSphere
- access to via console **388**
- version number **61**

SecureSphere Agent for DB2 z/OS
- IPv6 **54**

SecureSphere Agent for DB2 z/OS listeners
- defining on same port with Remote Agent listener **77**, **78**, **79**, **125**, **174**

SecureSphere configuration
- importing and exporting **262**

SecureSphere data
- listing contents of exported file **265**

Security Policy
- comments **321**

security world **402**

sessions
- killing **245**
- sticky **343**

SFTP
- connecting as unprivileged user **57**

SHA-2 **57**

SharePoint
- installing Remote Agent **124**

shell sessions
- timeout **58**

shutdown **455**

silent installation
- Windows agents **129**
- Windows Remote Agent **132**

silent uninstall
- Remote Agents **142**

Single Sign On **112**

size limits
- profiles **288**

Sniffing **215**

SOAP actions
maximum per URL **290**, **291**

source applications
maximum per user **288**

source IP addresses
maximum per user **289**

source OS users
maximum per user **289**

SOX report **318**

SSH
login to appliance using **56**, **57**, **59**

SSH proxy
scans **317**

SSL **30**, **112**

SSL accelerator cards **336**, **400**

SSL keys
deleting **300**
expiration **300**

SSO **112**

static routes
IPv6 **89**
VRRP **54**

sticky sessions **343**

stored procedures
definition of "built-in" **323**

STP **102**
and High Availability **74**
configure on a bridge **74**

STP Bridge **215**, **216**

sub-directories
maximum per directory **290**

SUSE **122**
Remote Agents **130**

swinstall **124**

syslog **56**, **57**, **217**
OS date command **58**

system date
administrator notified when changed **58**

system event
profile size violation **288**

system password **263**, **264**, **265**, **266**, **267**

T

TCP **147**

TCP reset **37**

teardown **99**

Teradata **319**

ThreatRadar
enabling and disabling **326**
IPv6 **52**

using a proxy **306**

time zone **91**

timeout
shell sessions **58**

top command
Linux **330**, **335**

Transparent Reverse Proxy
configuring **102**
description **30**

Transparent Reverse Proxy rule
conflict **102**

troubleshooting **335**

TRP
FIPS 140 compliance **460**

TZ format **91**

U

UDP **126**, **147**
LSO **161**

UDP checksum **217**

uninstall
Remote Agents **142**

Universal User Tracking **394**

unlocking a user **95**

UPS **41**

URL pattern **288**

URLs
maximum per application **290**
maximum per directory **289**

URM
audit enrichment **306**

users
disabling **245**
locking **95**
managing **84**
unlocking **95**

UTF8 **306**

V

version number
SecureSphere **61**

virtual instance **151**

virtual IP **126**

virtual IP mask **150**

virtual route **127**

virtual router **150**

VMware
Remote Agents **154**

VRRP **150**
configuring routes **100**
deprecated commands **54**

gateways in same subnet **100**
High Availability **108**
IPv6 **54**
KRP **106**
listeners **99**
static routes **54**

VT 100 **388**

W

Web scanners
using a proxy **306**

web to database user tracking
parameters **296**

winpcap **124**

WinSCP **57**

wizard
Remote Agent configuration **137**