nFX Log One and netForensics Reporting User Guide

Version 6.0

nFX Log One

netForensics, Inc.
200 Metroplex Drive
Edison, NJ 08817
732.393.6000
732.393.6025 (Fax)
732.393.6060 (International Support Line)
Email: support@netforensics.com
Online Request: http://support.netforensics.com
www.netForensics.com

nFX Log One and netForensics Reporting User Guide
Version 6.0
Build: 123107

© 2007 netForensics, Inc. All rights reserved. netForensics, the netForensics Logo, nFX, nFX OSP, nFX Data One, nFX Log One, nFX SIM One are registered trademarks of netForensics Inc. All other trademarks and servicemarks used in this document are the property of their respective companies. Customers may make reasonable numbers of copies of this publication for internal use only. This publication may not otherwise be copied or reproduced, in whole or in part, by any other person or entity without the express written permission of netForensics, Inc.

Oracle 9i is a registered trademark of Oracle Corporation
Cisco is a registered trademark of Cisco Systems, Inc.
Check Point, FireWall-1, and *OPSEC* are trademarks or registered trademarks of Check Point Software Technologies, Ltd.
Entercept is a registered trademark of Network Associates, Inc
RealSecure is a registered trademark of Internet Security Systems
Red Hat Linux is a registered trademark of Red Hat
UNIX is a registered trademark of The Open Group
Java, *Sun*, and *Solaris* are trademarks or registered trademarks of Sun Microsystems, Inc.
Microsoft, *Windows NT*, *Windows 2000*, and *Internet Explorer* are trademarks or registered trademarks of Microsoft, Inc.

Disclaimer: The information contained in this document may change without notice, and may have been altered if you have received it from a source other than netForensics, Inc. Use of this information constitutes acceptance for use in an 'AS IS' condition, without warranties of any kind, and any use of this information is at the user's own risk. netForensics, Inc. disclaims all warranties, either expressed or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall netForensics, Inc. be liable for any damages, including direct, indirect, incidental, consequential, or special damages arising from the use or dissemination hereof. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages, so the foregoing limitation may not apply.

Reference to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by netForensics, Inc. The views and opinions of authors expressed do not necessarily state or reflect those of netForensics, Inc. and shall not be used for advertising or product endorsement purposes.

Links and addresses to Internet resources are inspected thoroughly prior to release, but the changing nature of the Internet prevents netForensics, Inc. from guaranteeing the content or existence of the resource. If you find a broken or inappropriate link, please send an email with the topic name, link, and its behavior to: support@netforensics.com

December 2007

Contents

Overview 5
Who Should Read This Document 5
Document Conventions 5
Related Documents 6
Contacting netForensics Technical Support 6
Getting Started with nFX Log One 7
System Requirements 7
Installing nFX Log One 7
nFX Log One Licensing 8
Viewing Current License Information 8
Updating the nFX Log One License File 8
Uninstalling nFX Log One 8
Uninstalling Agents 8
Uninstalling nFX Log One Server Components 9
Getting Started with netForensics Reporting 10
netForensics Reporting Prerequisites 10
SQL 2005 Reporting Services 10
SQL Reporting Services Product Information 11
System Requirements 11
Prerequisites and Installation Tips 11
SQL 2000 Reporting Services 10
SQL Reporting Services Product Information 12
System Requirements 12
Prerequisites and Installation Tips 12
Installing netForensics Reporting 13
netForensics Risk Assessment 16
Getting Started with nFX Log One 17
nFX Log One Management Console 17
Logging In to the nFX Log One Management Console 17
Logging Out of the nFX Log One Management Console 18
Installing a Remote nFX Log One Management Console 18
Web Console Configuration 19
Checking the Version of nFX Log One 20
nFX Log One's Setup Utility 21

Installing nFX Log One Agents 22
Remote Agent Installation 22
Creating User Accounts 23
Configuring Corrective Actions 25
User Profile Properties 26
Personal Information 26
Notification Schedule 26
Message Format 27
Dialup Pager & SMS Options 28
Creating Business Groups 29
Business Group Properties 30
Audit Settings 31
Privileges 31
Deployment Options 32
Event Routing Configuration 33
E-mail Tab 33
Generic Dialup Pager Tab 34
SNMP Traps Generator Tab 35
Log Management and Archiving 36
Log Archiving 37
Event Log Management 38
Syslog Management 39
Third Party Log Management 40
Validating and Viewing Encrypted Logs 40
Log Management Configurations from Web Console 44
Event Watcher 45
Using Rules in Event Watcher 45
Viewing Live Events in the nFX Log One Console 46
Customizing the Live Event Watcher 47
Event Watcher Rules 48
Creating an Event Watcher Rule from a Live Event 48
Using the Event Watcher Rule Description Pane 49
Using the Event Watcher Rule Functions 50
Rule Criteria Based on Header 50
Event Watcher Rule Options 51
Action Taken on Event Match Option 51
Corrective Action Selection Option 52
Event Acknowledgment Option 52

Event Routing Information Option 52
Frequency of Notification Option 54
Message Text Option 54
Notification Schedule Option 55
Priority of Notification Option 55
Resolution Option 56
Text Based Rules Option 56
Creating a New Custom Event Watcher Rule 57
SysLog Watcher 58
Creating a SysLog Watcher Rule 59
Basic Syslog Settings 60
Performance Watcher 62
nFX Log One Performance Watcher 62
Configuring Performance Watcher Alerts 62
To Configure a Performance Watcher Template 63
To Configure the Server Update Frequency 63
Creating an Application Template 64
To Create a New Application Template 64
Defining the Performance Threshold 64
Collection 65
To Configure Default Performance Counter Properties 66
Applying Performance Templates to Systems 67
Using the Live Performance Watcher 67
To Edit the Properties of the Live Graph 68
To Delete a Counter from the Graph 69
To Save a Live Graph 69
To Open a Saved Performance Chart 69
To Change Performance Report Time Period 69
Text File Watcher 69
Creating a Text File Watcher Rule 70
Saving and Importing a Text File Watcher Template 77
nFX Log One System Management Tools 78
System Management Tool Overview 78
Snooze Tool 78
Configuring a Snooze 79
To UnSnooze a System 83
Changing the Properties of a Scheduled Snooze 84
Reboot Tool 85

Changing the Properties of a Scheduled Reboot 88
Run Tool 88
Changing the Properties of a Scheduled Task 92
Scheduler 92
Service Control Manager 93
Alert Maintenance Tool 94
Database Configuration Tool 95
Changing Database Repositories 95
Database Quota Management Tool 96
Backup and Restore Tool 97
Backing Up an nFX Log One Configuration 97
Restoring an nFX Log One Configuration 98
Utilizing Reports in netForensics Reporting 99
Report Execution 99
Exporting Reports 102
Message Text Searching 103
Report Configuration 104
Saving Reports 104
Moving Reports 104
Deleting Reports 106
Changing Company Logos in a Report 106
Changing the Data Source DSN settings 107
Report History 109
Report Subscription 109
Report Access and Role Assignments 112
Notes: 115

Overview

It's time to take control of log management.

nFX Log One not only gives you unprecedented access to your logs, but also simplifies compliance requirements to securely store, review and report on event logs. Most low-cost log management solutions lack the extended features and automated capabilities you need - and highly-featured solutions tend to be either too expensive or difficult to deploy. nFX Log One is the single answer to these challenges.

Welcome to nFX Log One and netForensics Reporting -- your new, state-of-the-art solutions for protecting the integrity of your enterprise data by monitoring and consolidating security event logs on all systems, databases, and devices. nFX Log One and netForensics Reporting deliver the most intuitive security and compliance reporting system available in today's marketplace.

nFX Log One will help your enterprise prove that internal controls are in place and effective, access to financial data is controlled and reported on, and steps have been taken to meet various regulatory compliances such as those required by Sarbanes-Oxley.

netForensics Reporting is a flexible, full-featured web-based reporting suite, which utilizes 'best of breed' technology and delivers a host of pre-defined security events, systems management, and performance reports as well as specific compliance reports for Sarbanes-Oxley, Gramm Leach-Bliley, and HIPAA, etc.

The *nFX Log One and netForensics Reporting User Guide* will help you understand both the basic and advanced functionality of these two exciting products so that you can take advantage of the powerful functionality that both products have to offer. nFX Log One and netForensics Reporting put the power of protecting the integrity of your enterprise data into your hands.

Who Should Read This Document

This guide provides details about the deployment and usage of nFX Log One version 6.0 and netForensics Reporting. It is designed for users and analysts who monitor security networks.

For general information about network security, see the documents available from the netForensics Resource Web page at:

http://www.netforensics.com/resources/

Document Conventions

The following text conventions are used in this document:

- Menu items, button names and commands appear in **bold**.
- Paths in the software appear in smaller, ***bold italic*** text.
- New or important terms and document titles appear in *italics.*
- Text that you see on the screen appears in a `screen font`.
- Variables appear between brackets in an italic screen font: `<variables>`
- Command input and file names appear in a **`bold screen font`**.
- Variables for which a value is required appear between brackets in a bold italic screen font: ***`<file name>.`***
- The **Start>Run** option represents clicking the **Start** button on the Taskbar, and then clicking **Run** from the pop-up menu.
- When typing commands, you must press **[Enter]** to invoke any command, even if you are not expressly told to do so.
- The **#** and **$** symbols denote the Linux command prompts for user **root** and non-root users.

Related Documents

Other documents that may be useful:

- *nFX Log One V 6.0 Release Notes*
- *nFX Log One V 6.0 Troubleshooting Agent Deployment Guide*

Contacting netForensics Technical Support

netForensics Technical Support can provide technical documentation and personal assistance to answer any questions you may encounter while using nFX Log One. You can reach netForensics Technical Support in any of the following ways:

1. **Telephone** (Monday through friday from 7 a.m. to 10 p.m. EST)

   International Support Line:

   1.732.393.6060

   North America Support Line (Toll Free):

   1.866.9NFX.HELP (1.866.963.9435)

2. **Email**

   support@netforensics.com

3. **Online Requests**

   http://support.netforensics.com

Getting Started with nFX Log One

In this section, you will learn about the nFX Log One's installation requirements and processes. You will also learn about:

- System Requirements
- Installing nFX Log One
- nFX Log One Licensing
- Uninstalling nFX Log One

System Requirements

Before installing nFX Log One please ensure that all OS hardware requirements have been met. nFX Log One is designed to work best under the conditions listed below:

	nFX Log One Server	SQL Server 2000/2005	Agents	Management Console
Operating System	Windows 2000, 2003, XP	Windows 2000, 2003, XP	Windows NT 4.0, 2000, 2003, XP (32 and 64 bit)	Windows 2000, 2003, XP
OS Type	Server, Workstation	Server, Workstation	Server, Workstation	Server, Workstation
Platform	Intel	Intel	Intel	Intel
RAM	2 GB	2 GB	1 GB	1 GB
Hard Disk Space	5+ GB minimum free hard disk space	10+ GB minimum free hard disk space	1+ GB minimum free hard disk space	1+ GB minimum free hard disk space
System Speed	Pentium IV 2+ GHz	Pentium IV 2+ GHz	Pentium IV 1+ GHz	Pentium IV 1+ GHz

Table 1: nFX Log One System Requirements

Important

SQL Server 2005 is recommended over SQL Server 2000 because SQL Reporting Services are built into the installation of SQL Server 2005.

Important

Disk space requirements may vary depending on the number of events generated by monitored computers and the type of filtering strategies used. Keep in mind that the non-filtering of events could increase the amount of disk space required for computers generating thousands of events per day. In addition, log backup and purging schedules will play an important role in determining your actual disk space requirements.

Installing nFX Log One

nFX Log One is installed via a standard **InstallShield Wizard**. During the installation process, you will be prompted to provide the following information:

- User name, company name, and serial number (provided by netForensics)
- Your choice of SQL Server to serve as the nFX Log One Database
- Destination drive and folder location for nFX Log One system files

- SQL Server name
- SQL Server admin account with password
- nFX Log One Database name

Important

Keep in mind that the computer on which you are installing nFX Log One automatically becomes the nFX Log One Server. The nFX Log One Database is automatically created during the installation process.

nFX Log One Licensing

nFX Log One's licensing structure *controls* the number of **Servers**, **Workstations**, and **Devices** (any **Syslog** sources) where your nFX Log One software can be installed. It also controls the expiration date of your license(s).

Important

The **nFX Log One License File** will be sent to you via e-mail and should be copied onto your hard disk for safe keeping.

Viewing Current License Information

Information regarding the number of Servers and Workstations that your copy of nFX Log One is licensed for and how many Workstations and Servers are currently deployed can be viewed by following the steps:

1. Open the **nFX Log One Console** and select ***Help > About netForensics nFX Log One***.
2. Select the **License Information** tab. Here you can also view the expiration date of your **nFX Log One license**.

Updating the nFX Log One License File

A new **License File** can be uploaded into nFX Log One by accessing the License Update screen.

1. Open the **nFX Log One Console** and Select ***Help > About netForensics nFX Log One***.
2. Select the **License Information** tab.
3. Select the **Update License** tab to locate and upload a new license file for nFX Log One.
4. Once the new license is accepted, a **License Update Successful** pop-up message displays. The new license information will not be displayed until you reopen the licensing interface.

Uninstalling nFX Log One

Uninstalling Agents

In order to uninstall the **nFX Log One Agent software**, you must first access the **nFX Log One Setup** interface.

1. Select ***Go > Setup*** from the **nFX Log One Console** toolbar.
   - » The **Setup** screen displays.
2. Click on the **+** sign next to the **Business Group** in the upper left window pane where the agent resides. **Note:** All agents are added to the **Enterprise Group** by default.
3. Right click the computer name

4. Select **Delete**.

Important

The actual removal of the software will take place the next time the **nFX Log One Agent** checks in with the **nFX Log One Server**.

Uninstalling nFX Log One Server Components

In order to uninstall nFX Log One from your computer, you must first uninstall the **nFX Log One Agent software** (see above) from any computers where it has been deployed. Once you have removed the **nFX Log One Agent software**, follow the steps below to remove the nFX Log One from your computer:

1. Select **Add or Remove Programs**.
2. Locate **nFX Log One** from your list of programs.
3. Highlight **nFX Log One** from the list.
4. Select **Remove Program**.
   - » nFX Log One is now removed from your computer.

Getting Started with netForensics Reporting

This section will help you ensure a successful **netForensics Reporting** implementation. Please review this section carefully as it will provide you with the information that you'll need to get the most out of your netForensics Reporting software. This section covers the following topics:

- netForensics Reporting Prerequisites
- Installing netForensics Reporting
- netForensics Risk Assessment

netForensics Reporting Prerequisites

In order to install netForensics Reporting, you ***must*** have **SQL 2000 Reporting Services** running on the same computer where you want to install netForensics Reporting. You can verify that **SQL 2000 Reporting Services** is running and working properly on your computer by opening the **SQL 2000 Reporting Services** default home page. (**`http://machine_name/reports`**)

1. From the Windows Desktop, select ***Start > Programs > Microsoft SQL Server > Reporting Services > Report Manager.***

   » The **SQL Reporting Services** default home page displays.

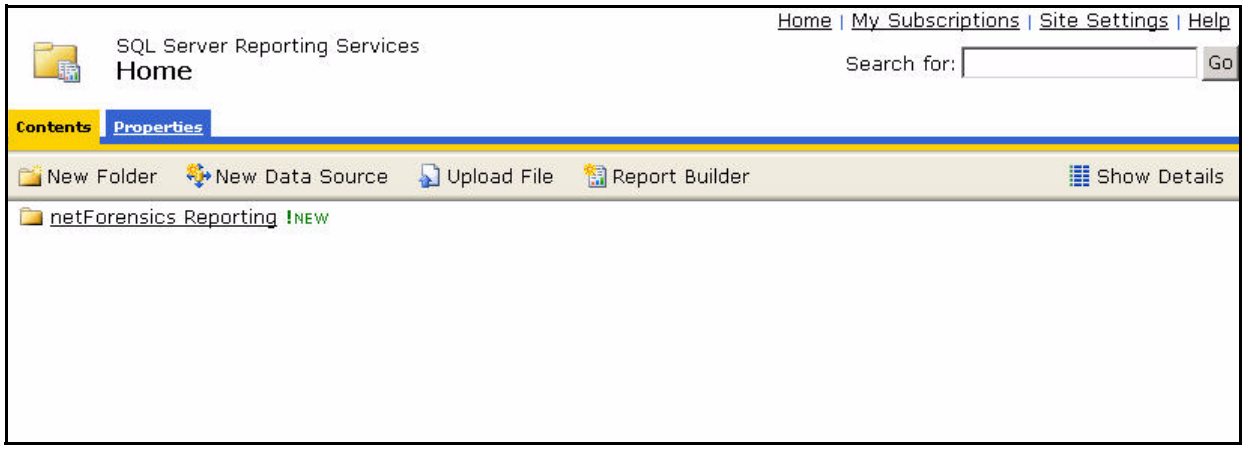


Figure 1: SQL Server Reporting Services screen

Important

netForensics Reporting requires **.NET Framework 2.0** to be installed prior to the installation.

SQL 2005 Reporting Services

Microsoft SQL 2005 Reporting Services can be installed on computers that do not already have MS SQL Server installed.

Important

A **Product Key** is not required if you are installing **MS SQL 2005 Reporting Services** on a **MS SQL Server**. Below you will find links to Microsoft's SQL Reporting Services web sites, which will provide you with additional information.

SQL Reporting Services Product Information

Click on the link below to review **Microsoft's SQL Server Reporting Services Product Information** web page: SQL Reporting Services Product Information.

System Requirements

To review Microsoft's minimum system requirements to run **SQL Reporting Services**, click on the following link: System Requirements.

Prerequisites and Installation Tips

Below is a list of prerequisites necessary to install **MS SQL 2005 Reporting Services**.

- The **MS SQL 2005 Reporting Services** installation computer must be running IIS 5.0 or later with the **World Wide Publishing** option enabled.
- The **MS SQL 2005 Reporting Services** installation computer must have **.Net Framework 2.0** or later installed and it must be installed after IIS has been installed.

Important

During the installation of **MS SQL 2005 Reporting Services** you will be prompted to accept or enter information at various times during the process. Below are a few tips to assist you during the installation.

- Install **MS SQL 2005 Reporting Services** using most of the default settings.
- Use either your **SQL 'sa' account** information or **Windows credentials** for connecting to the **SQL Server**.
- **Uncheck the SSL option**, if necessary.

Important

If you encounter an error loading the initial **MS SQL 2005 Reporting Services** default home page, **.NET Framework** may need to be registered again with IIS.

The following procedure will re-register **.Net Framework** and restart **IIS**.

1. Open a Command line screen and change directories to:

   ```
   C:\Windows\Microsoft.NET\Framework\v2.0.50727
   ```

2. Enter the following:

   ```
   aspnet_regiis.exe -i
   ```

3. Enter:

   ```
   iisreset
   ```

Tips and Reminders

Important

For automated scheduled subscription reporting, set the **MS SQL 2005 Agent Service Start-up** option to *automatic*.

Important

Add the **MS SQL 2005 Server Reporting Services** default home page to the **Trusted Sites** setting in **Internet Explorer (IE)**.

SQL 2000 Reporting Services

Microsoft SQL 2000 Reporting Services can be installed on computers that do not already have MS SQL Server installed, however you will be required to enter a *Product Key* for MS SQL 2000 Reporting Services during the installation process.

Important

A **Product Key** is not required if you are installing **MS SQL 2000 Reporting Services** on a **MS SQL Server**. Below you will find links to Microsoft's SQL Reporting Services web sites, which will provide you with additional information.

SQL Reporting Services Product Information

Click on the link below to review **Microsoft's SQL Server Reporting Services Product Information** web page: SQL Reporting Services Product Information.

System Requirements

To review Microsoft's minimum system requirements to run **SQL Reporting Services**, click on the following link: System Requirements.

Prerequisites and Installation Tips

Below is a list of prerequisites necessary to install **MS SQL 2000 Reporting Services**.

- The **MS SQL 2000 Server instance** referenced during the installation must be updated to Service Pack 3a.
- The **MS SQL 2000 Reporting Services** installation computer must be running IIS 5.0 or later with the **World Wide Publishing** option enabled.
- The **MS SQL 2000 Reporting Services** installation computer must have .Net Framework 1.1 or later installed and it must be installed after IIS has been installed.

Important

During the installation of **MS SQL 2000 Reporting Services** you will be prompted to accept or enter information at various times during the process. Below are a few tips to assist you during the installation.

- Install **MS SQL 2000 Reporting Services** using most of the default settings.
- Use either your **SQL 'sa' account** information or **Windows credentials** for connecting to the **SQL Server**.
- **Uncheck the SSL option**, if necessary.

Important

If you encounter an error loading the initial **MS SQL 2000 Reporting Services** default home page, **.NET Framework** may need to be registered again with IIS.

The following procedure will re-register **.Net Framework** and restart **IIS**.

1. Open a Command line screen and change directories to:

   ```
   C:\Windows\Microsoft.NET\Framework\v2.0.50727
   ```

2. Enter the following:

   ```
   aspnet_regiis.exe -i
   ```

3. Enter:

```
iisreset
```

Tips and Reminders

Important

For automated scheduled subscription reporting, set the **MS SQL 2000 Agent Service Start-up** option to *automatic*.

Important

Add the **MS SQL 2000 Server Reporting Services** default home page to the **Trusted Sites** setting in **Internet Explorer (IE)**.

Installing netForensics Reporting

You can download the **netForensics Reporting installation** files from the netForensics web site. The installation process is easy and intuitive as once the process begins folders and canned reports are automatically created off the root **MS SQL Reporting Services** home directory. The following steps will help you with the installation of netForensics Reporting:

1. The **Choose Destination Location** screen displays. Here you can select the **SQL Server** folder where you would like Setup to install the netForensics Reporting files.
2. Select the **MS SQL Server instance** from the SQL Server List that contains the nFX Log One Database or select **Other** to manually enter the **SQL Server Instance** name.

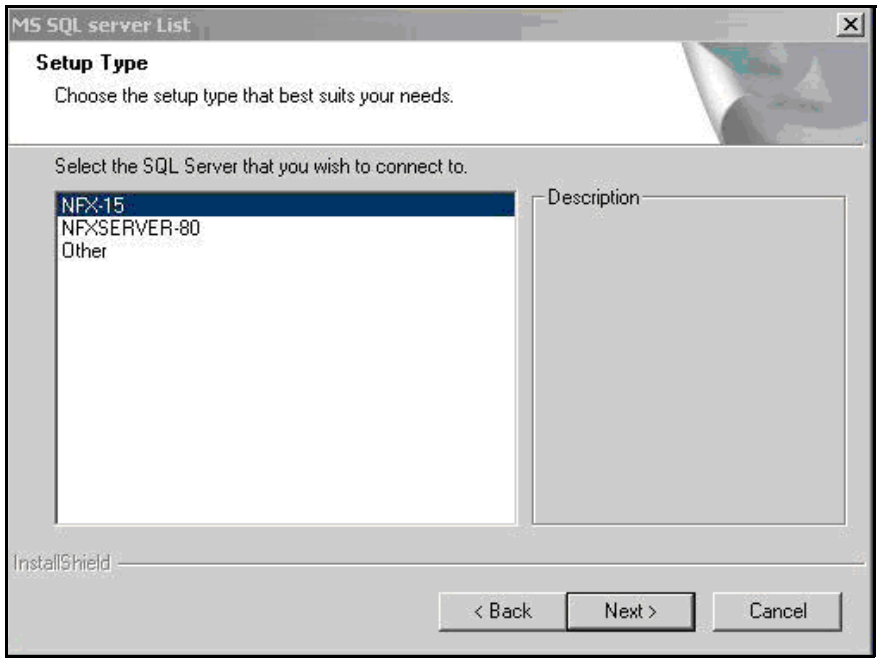


Figure 2: SQL Server List

3. Click **Next**.

» The nFX Log One Database Server Information screen displays.

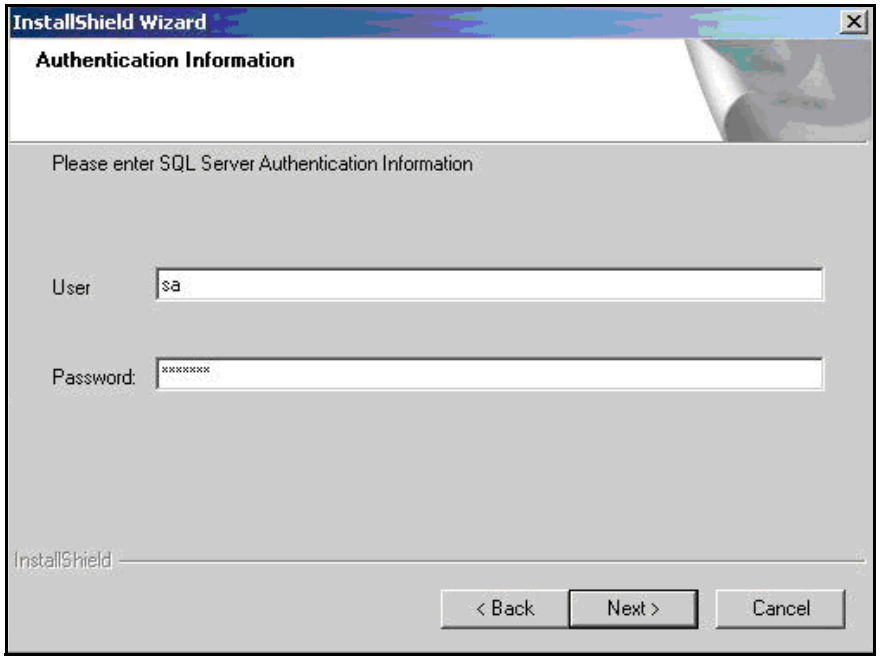


Figure 3: nFX Log One Database Server Information screen

4. Enter your **SQL Server Admin account** and **password**.
5. Click the **Next** button.
6. Enter the **nFX Log One Database Name**.

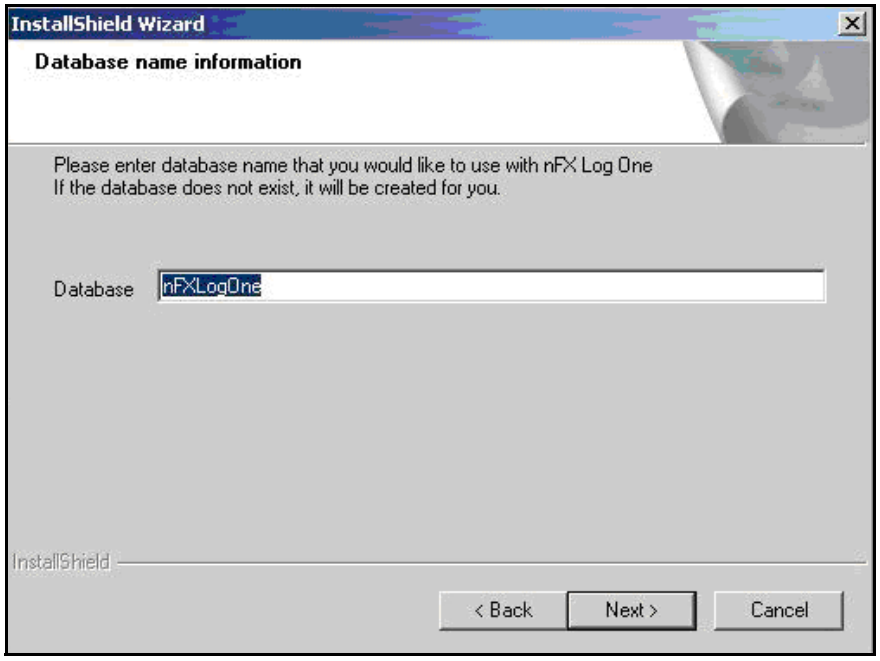


Figure 4: nFX Log One Database name Information screen

7. Click the **Next** button. Here, you are promoted to publish reports.

8. Verify that the netForensics Reporting folders and reports exist by browsing through the Report Folders as shown below.

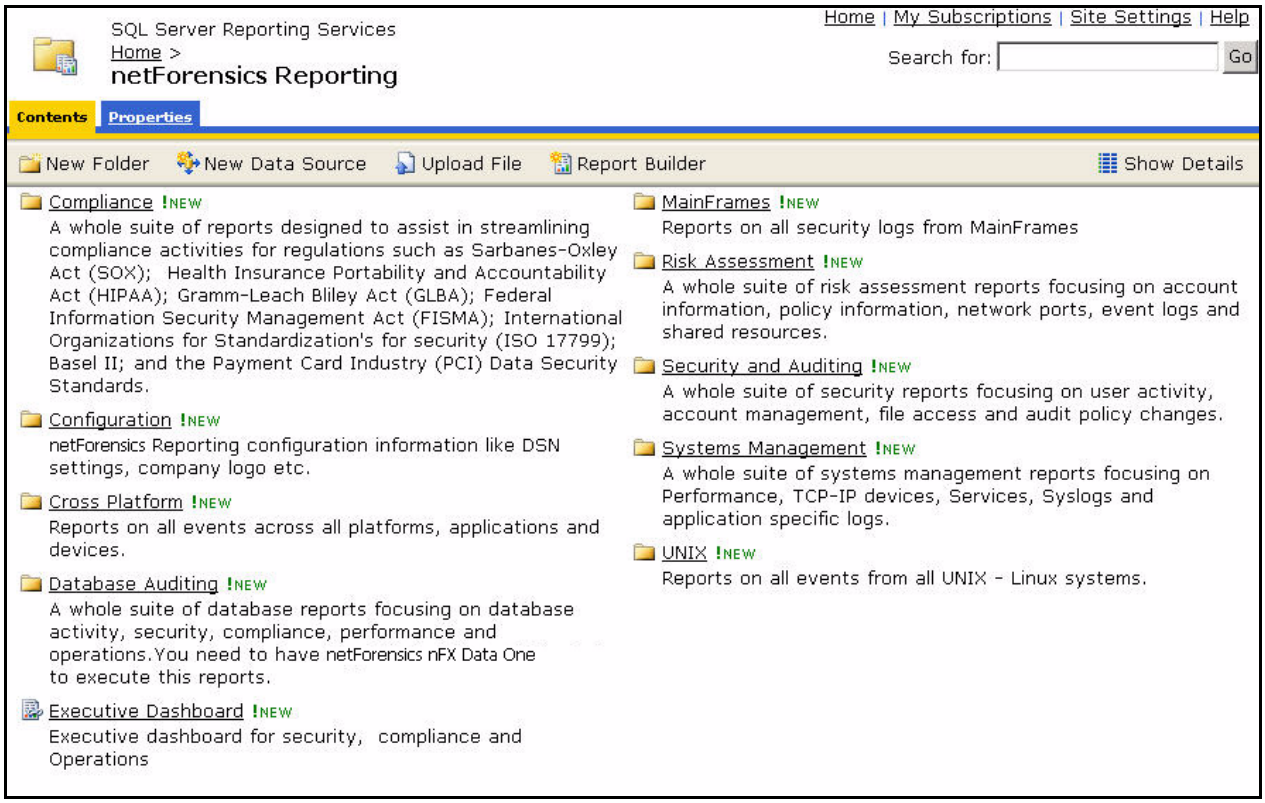


Figure 5: SQL Server Reporting Services home page

netForensics Risk Assessment

netForensics Risk Assessment components are installed by default when you install **netForensics Reporting version 6**. Previous versions required netForensics Risk Assessment to be installed after a successful installation of netForensics Reporting.

Important

You can easily verify that netForensics Reporting is working properly by opening the **netForensics folder** from the default SQL Reporting home page.

1. From Windows Start menu, select ***Start > Programs > netForensics > Reporting > Report Manager.***
   - » The **SQL Reporting Services** home page displays.

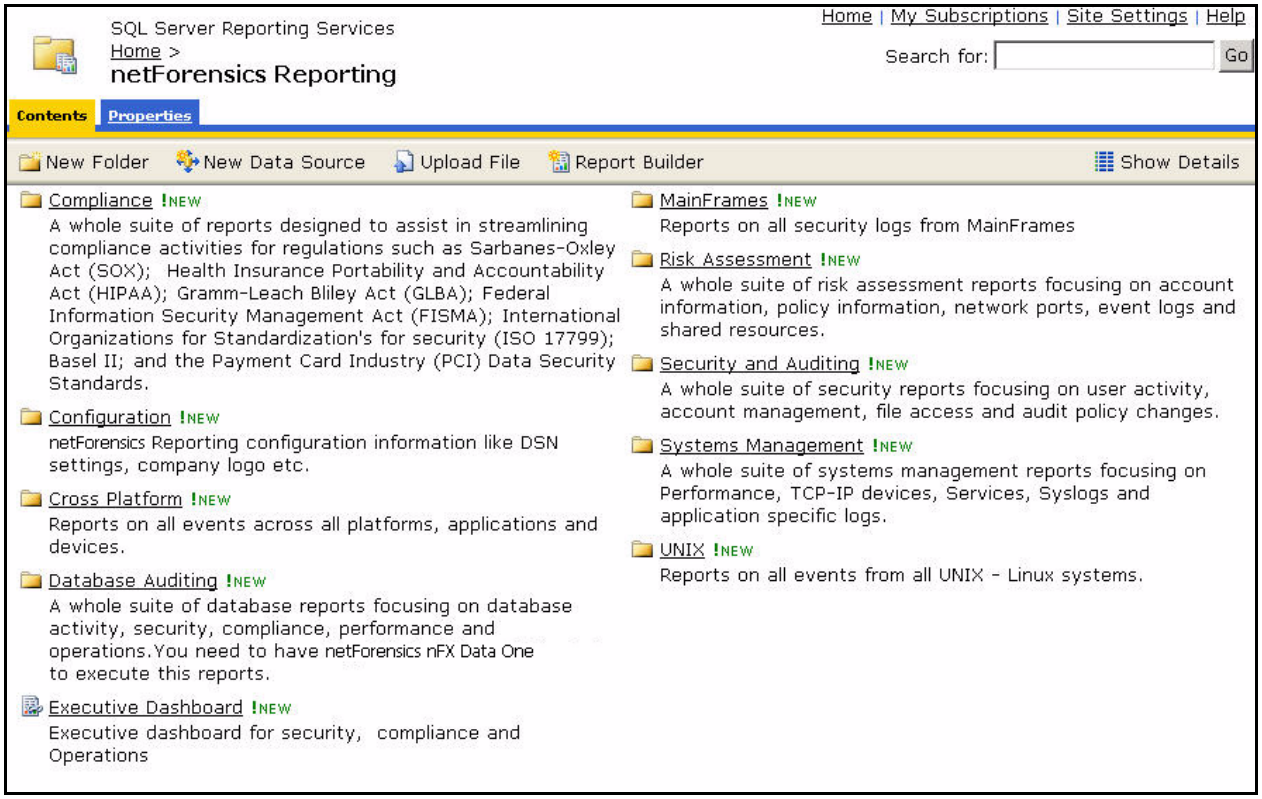


Figure 6: SQL Reporting Services home page

Getting Started with nFX Log One

Welcome to **Getting Started with nFX Log One**. In this section you will be introduced to the **nFX Log One Management Console User Interface**, learn how to log in and out of the nFX Log One Management Console, and learn how to install remote nFX Log One Management Consoles. You will also learn how to:

- Navigate the nFX Log One Setup Window
- Install the nFX Log One Agent
- Configure New nFX Log One Users
- Configure nFX Log One Groups
- Configure Corrective Actions
- Configure Event Routing
- Understand the nFX Log One Environment Variables for Batch Files

nFX Log One Management Console

The nFX Log One Management Console is an important part of your nFX Log One software as this is where all nFX Log One functionality is configured, managed, and monitored. The nFX Log One Management Console provides you with a single, consolidated interface for viewing the information collected by the nFX Log One Agents.

Logging In to the nFX Log One Management Console

Once nFX Log One has been installed, you can log into the nFX Log One Console using the steps below:

1. From the Windows Start menu, select ***Start > Programs > netForensics >nFX Log One > Management Console***.

   » The **nFX Log One** Login screen displays.

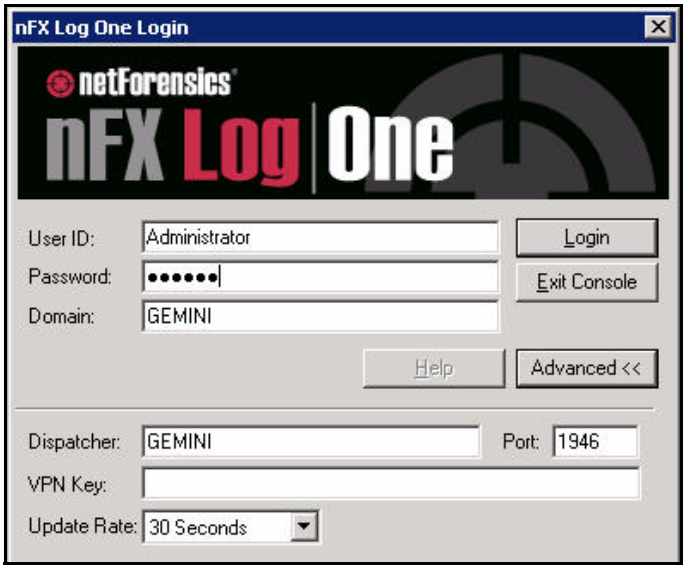


Figure 7: Management Console Login screen

2. Enter your **User ID** into the **User ID** field.
3. Enter your **Password** into the **Password** field.

4. Verify and/or enter the **Domain**.
5. Click **Login**.

Important

nFX Log One will attempt to fill in as many fields as possible based on your Windows settings and configuration as well as the information provided by the last user logged into nFX Log One. Therefore, it is important to review the data in any pre-filled fields and edit as necessary.

Important

The **Advanced >>** button located on the bottom right side of the nFX Log One Login screen expands the nFX Log One Login screen and gives you the ability to further define your login parameters. The fields located on the nFX Log One Login screen are described below:

Field Name	Description
User ID	Determines which privileges you have within the nFX Log One Management Console.
Password	The Windows password for the user ID you entered.
Domain	The Windows domain name where your user ID resides. Leave this field blank if your computer is part of a Workgroup.
Dispatcher	The Windows domain name for the nFX Log One Server computer.
Port	The port used by the nFX Log One Server to handle nFX Log One Management Console requests.
VPN Key	Virtual Private Network (VPN) Leave this field blank to use nFX Log One's internal 128bit blowfish encryption key.
Update Rate	Determines how frequently information is updated in the nFX Log One Management Console.

Table 2: nFX Log One Login screen descriptions

Logging Out of the nFX Log One Management Console

Once you are through using nFX Log One, you must log out. The steps below will instruct you on the log out process.

1. From the nFX Log One toolbar, click the **Logout icon**, or close all nFX Log One screens and select ***Go > Logout*** from the nFX Log One menu.
   - » The **nFX Log One Management Console** closes.

However, keep in mind that all of the nFX Log One Agents as well as the nFX Log One Server will continue to run as services in the background.

Installing a Remote nFX Log One Management Console

Installing a remote nFX Log One Management Console enables an Administrator to monitor and configure all nFX Log One features from any Intel-based computer running Windows NT 4.0/2000/2003/XP, no matter its physical or network location. The steps below will instruct you on how to install a Remote nFX Log One Management Console.

1. From the nFX Log One toolbar click the **Setup icon** or select ***Go > Setup*** from the nFX Log One menu.
2. In the **Network Browser** pane under the **Monitored Systems** Header, select the System Name on which you would like to install a remote nFX Log One Management Console. Or, you can simply **right-click** on the **Monitored Systems Header** and select ***New > Computer***.

   » **The Deploy to New Computer** dialog box displays.

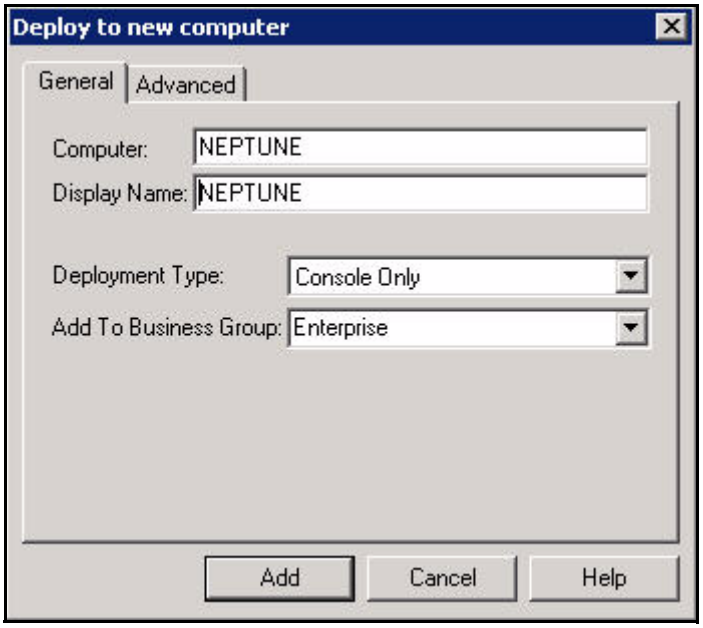


Figure 8: Deploy to New Computer dialog box

3. In the **Deploy to New Computer** dialog box, **General** tab enter the **Computer Name** in the **Computer** field.
4. Enter the **Display Name** in the **Display Name** field. Or, if the Display Name field and Computer Name field are already populated, simply verify that the information is correct.
5. Click on the **Deployment Type** drop-down menu.
6. Select **Console Only**.
7. Apply your changes by clicking the **Add** button located at the bottom.

Important

nFX Log One will deploy the necessary files to run the Remote Management Console. You can locate the **Console.exe** file in the ***c:\Program Files\netForensics\nFX Log One\bin*** directory.
It is recommended to create a shortcut for this file. Click the **Advanced** button and enter the **nFX Log One Server** name in the **Dispatcher** field and change the **Update Rate** to 30 seconds.

Web Console Configuration

In order to configure the nFX Log One Web Console, you must access it from the nFX Log One Management Console. The steps below will show you how to complete that task.

1. Open the nFX Log One Management Console from Windows ***Start > All Programs > netForensics > nFX Log One > Management Console***.
2. From the nFX Log One console menu, select ***Tools > Web Console Configuration.***

» The **Web Console Configuration** screen displays.

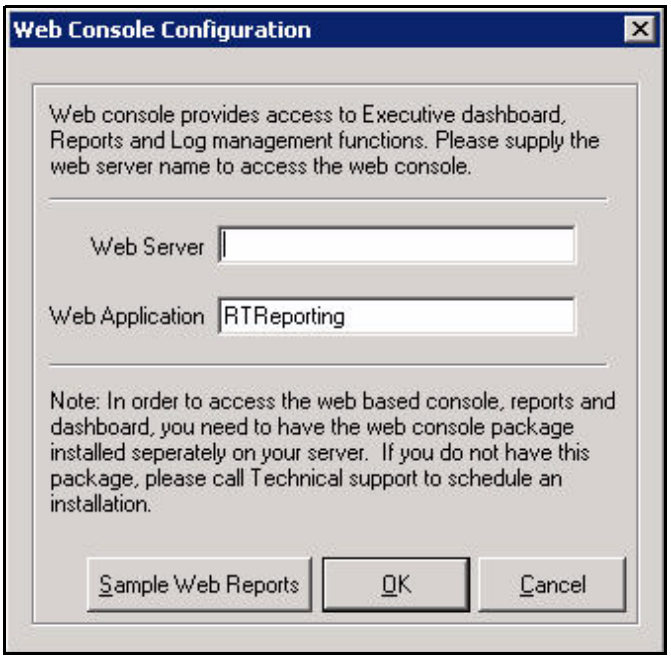


Figure 9: Web Console Configuration screen

3. In the **Web Server** field, enter the Web Server's **hostname** or **IP address** of the location of the **Web Console**.
4. The **Web Application** field always displays with **RTReporting**.
5. Click the **OK** button.

To access the **Web Console**:

1. From Windows, select ***Start > All Programs > netForensics > Reporting > Report Manager***.

Checking the Version of nFX Log One

If you would like to check to ensure that you have the latest version of nFX Log One:

1. From the nFX Log One console menu, select ***Help > Check for updates***.

» If you have the most current version of nFX Log One, the Information screen displays stating: Congratulations! You have the most current version of the product.

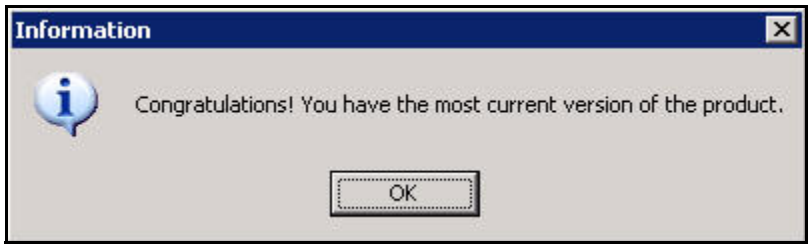


Figure 10: Version Information screen

Important

If you do not have the latest version, you will see a dialog box that says '**New Updates are Available**.' To get the new updates, go to your Client page on the netForensics Reporting web site or contact netForensics support.

nFX Log One's Setup Utility

The **nFX Log One Setup Configuration** interface provides you with easy, single-screen access to configure the base information nFX Log One requires specific to a single nFX Log One Server. This section will also discuss how to:

- Navigate the nFX Log One Setup Screen
- Install the nFX Log One Agent
- Configure New nFX Log One Users
- Configure nFX Log One Groups
- Configure Corrective Actions
- Configure Event Routing
- Use the nFX Log One Environment Variables for Batch Files

The nFX Log One Setup Configuration interface provides an easy, single screen access to configure the base information that nFX Log One requires that is specific to a single nFX Log One Server. To launch the nFX Log One Setup Configuration interface:

1. From the **nFX Log One Management Console** toolbar, click the **Setup icon** or select ***Go > Setup*** from the nFX Log One Console menu.

   » The **Setup** screen displays.

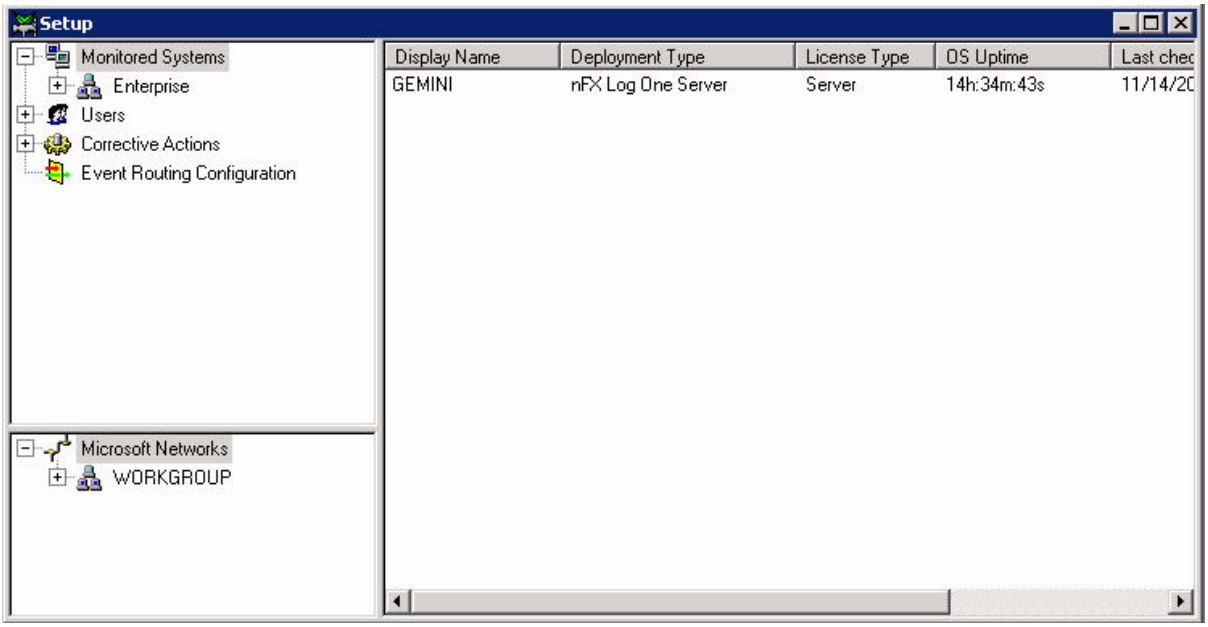


Figure 11: Setup screen

The Setup screen is divided into *three* panes.

1. The **Setup Configuration** section is located on the upper left pane of the Setup screen.

   In the upper left window pane of the Setup screen, you can right click on any of the text to add computers, users, and corrective actions.

2. The right pane of the Setup screen is *dynamic* and changes according to your Console refresh rate located in Advanced Settings on the Login screen.

3. The lower left pane displays information for Microsoft Networks and WORKGROUPs.

Installing nFX Log One Agents

nFX Log One Agent software must be deployed to a computer before the nFX Log One Server can manage this system. Once the nFX Log One Agent software is installed and running on a computer, the nFX Log One Agent root service will *immediately* begin sending Windows events back to the nFX Log One Server and store them in the nFX Log One database, based on the default set of nFX Log One Event Rules.

1. Start by executing one of the following:
   a. From the **Setup** screen, **right-click** on the **Monitored Systems header** and select ***New > Computer***.
   b. From the **Setup** screen, highlight the computer(s) in the **Network Browser** lower left pane, right-click, and select **Deploy Agent**.
   c. From the **Setup** screen, choose a computer from the **Network Browser** lower left pane and drag and drop it into one of the Business Groups listed in the Monitored Systems pane.
2. At the **Deploy to New Computer** dialog, you are required to confirm the name of the computer information and the preferred display name.
3. You are also required to identify the **Deployment Type** with options for **Agent Only**, **Agent with Console**, or **Console Only**.

Remote Agent Installation

In some instances, nFX Log One Administrators will want to install the nFX Log One Agent software on remote systems in a DMZ, through a firewall or on remote systems that may be locked down for security purposes.

Important

Please remove any instance of the agent machine listed in nFX Log One Setup prior to installing the 6.0 nFX Log One Agents remotely.

Important

nFX Log One 6.0 ships with one self contained MSI package for remote agent installations and upgrades. This package includes the **RemoteAgentSetup.msi** and the **Run_LC_Agent_Bootstrap.bat** located the **netForensics\nFX Log One\Tools\Remote Install** folder. This MSI package installation is compliant with MS-SMS or Altiris based software re-distribution applications.

The **MSI installer** has all the required agent files within the package. Follow the steps below:

1. First, you will need to uninstall previous versions of the nFX Log One Agent bootstrap from **Add/Remove Programs** using the following command:

   ```
   Msiexec /x agentbootstrap.msi /qn
   ```

2. Use the example command line shown below for installation.
3. Update the **Run_LC_Agent_Bootstrap.bat** file with the correct **IP address** of your nFX Log One Server.

Example:

```
msiexec /i remoteagentsetup.msi /qn LC_SERVER_IP=192.168.0.84
LC_SERVER_PORT=1945 LC_AGENT_FILES=local INSTALL_DRIVE_LETTER=c
BUSINESS_GROUP=Enterprise /lv msiinstall.txt
```

LC_AGENT_FILES is a new command line parameter. It can take any one of the following two values: "***Local***" or "***Remote***". **Local** uses the agent files, which are available in the package as opposed to the option **Remote** which downloads files from the nFX Log One server.

Important

You must enclose in double quotes **" "** if a **Business Group** contains a space in the middle.
For example, **"Domain Controllers"**.

Important

The installation will fail if this machine is already listed in **nFX Log One's Setup Monitored Systems** list. Remove the machine from **Setup** prior to installing **Remote Agent** software.

Important

If you are monitoring the remote computer through a firewall, you will need to ensure that TCP port 1945 is open for data communications to the nFX Log One Server from the IP address of the nFX Log One Remote Agent. To test communications, open a Command Line prompt on the remote agent machine and enter: **telnet nFX_Log_One_server_IP_address 1945**. Hit **<Enter>** twice to *verify communications*.

Creating User Accounts

nFX Log One's User Configuration option allows you to create and modify the users that are configured to administer nFX Log One. By creating a user, you can allow that user to be notified when certain events occur via user specific communication settings and time scheduling.

Important

By default the user ID that you logged into the computer with during the initial installation will be the only user ID that the nFX Log One Server will permit to log into the nFX Log One Management Console.

The following steps will show you how to create a **New User**. Be sure to include all of the information in the following steps as this will allow you to correctly route **Event Alerts** to this user.

1. **Right-click** on anywhere in the upper left pane of nFX Log One **Setup**.
2. Select ***New > User***.

» The **Add New User** dialog box displays.

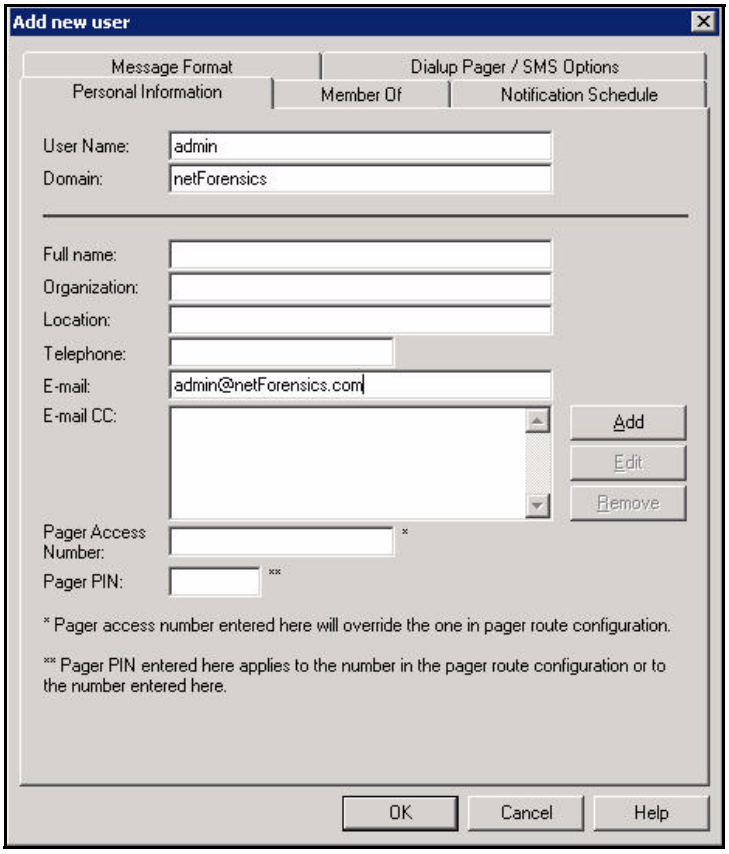


Figure 12: Add New User: Personal Information tab

3. Click the **Personal Information** tab.
4. Enter the **User Name** in the **User Name** field.
5. Enter the **Domain Name** in the **Domain Name** field.
6. Enter the User's **Full Name** in the **Full Name** field.
7. Enter the name of the User's **Organization** in the **Organization** field.
8. Enter the User's **Location** in the **Location** field.
9. Enter the User's **Contact Telephone Number** in the **Telephone** field.
10. Enter the User's **E-mail Address** in the **E-mail** field.
11. Enter additional **e-mail addresses** in the **E-mail CC:** field by clicking the **Add** button.
12. Enter the User's **Pager Number** in the **Pager Access Number** field.
13. Once you have entered all of the required information, click the **OK** button.

» A **New User** has been added.

Important

You can use the **Add** or **Remove** buttons on the **Personal Information** tab to include or exclude this user from certain Business Groups, which is discussed later in this section. Keep in mind that a single user CAN be a member of multiple Business Groups. Grouping users into Business Groups is a highly recommended method to simplify nFX Log One Administration.

Configuring Corrective Actions

nFX Log One allows you to pre-configure programs, batch files, or any script of your choice to be executed when certain events occur. As part of your nFX Log One setup, you must provide nFX Log One with a locational reference to any scripts or executable files that you have created. This will enable nFX Log One Agents or the nFX Log One Server to execute the file appropriately when called for in your Event Watcher Rules.

Important

It is important to understand that **Corrective Actions** are applied within the Event Watcher configuration, however the files associated with the Corrective Actions must first be defined in nFX Log One within the Setup Utility.

One Corrective Action executable file is included with nFX Log One for your use and is listed in the ***Setup > Corrective Actions*** tree. This file, **send_net_msg.bat**, launches a pop-up message on the console of selected users when called.

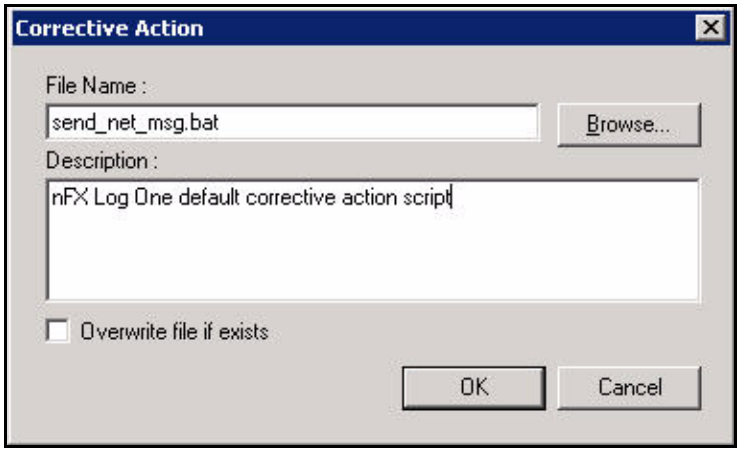


Figure 13: Corrective Action screen

Follow the steps below to add a Corrective Action file reference:

1. **Right-click** on the **Corrective Actions** header from within the nFX Log One Setup utility.
2. Select **New > Corrective Action** and find the corrective action file.

Important

Certain programs and scripts are written specifically for certain processors. Ensure that the program or script will work with the processor on the machine that will be deploying the script.

Important

nFX Log One allows the use of DCOM for corrective actions. However, you must install the MS Windows Scripting Host on the machine that will be running the Corrective Action script. When configuring a Corrective Action Selection in the Event Watcher filtering options, nFX Log One copies the script, program or batch file that is associated with that filter to the agent level when the rules are applied. The Corrective Action files reside in nFX Log One/bin/correctiveActions directory.

User Profile Properties

The following sections describes additional information as relates to user accounts. The following tabs are described below:

- Personal Information
- Notification Schedule
- Message Format
- Dialup Pager & SMS Options

These tabs can be located:

- When creating a new user, in the **Add new user** dialog box found by **right-clicking** in the upper left pane of the **Setup** screen and selecting ***New > User*** or,
- For existing users, in the **User Properties** dialog box found by **right-clicking** the user name in the upper left pane of the **Setup** screen and selecting **Properties**.

Personal Information

The nFX Log One **Personal Information** tab of the **Add new user** or **User Properties** dialog box allows you to view or modify user settings. See Figure 12 for more information.

1. In either the **Add new user** or **User Properties** dialog box, select the tab: **Personal Information**.
2. View or edit the text fields according to the following:

Field Name	Description
User Name	Name the user will use to login.
Domain	Domain of nFX Log One
Full name	Full name of the user.
Organization	Organization to which the user belongs.
Location	Location of the user.
Telephone	Telephone number of the user.
E-mail	E-mail address of the user.
E-mail CC	E-mail addresses to which e-mail notifications should be sent. Control this list by using the **Add**, **Edit** or **Remove** buttons.
Pager Access Number	Access number to the user's pager.
Pager PIN	PIN number for the user's pager.

3. When finished viewing or editing, click **OK**.

Notification Schedule

The nFX Log One **Notification Schedule** tab of the **Add new user** or **User Properties** dialog box allows you to determine the time of day and day of the week that the user will be considered working and therefore notification via email or pager should be sent. The highlighted hours are the hours during which the user will receive notifications.

1. In either the **Add new user** or **User Properties** dialog box, select the tab: **Notification Schedule**.
   - » The highlighted hours are the hours during which the user will receive notifications.
2. Use the **Toggle Working Hours** button to configure normal work hours and days.
3. When finished, click **OK**.

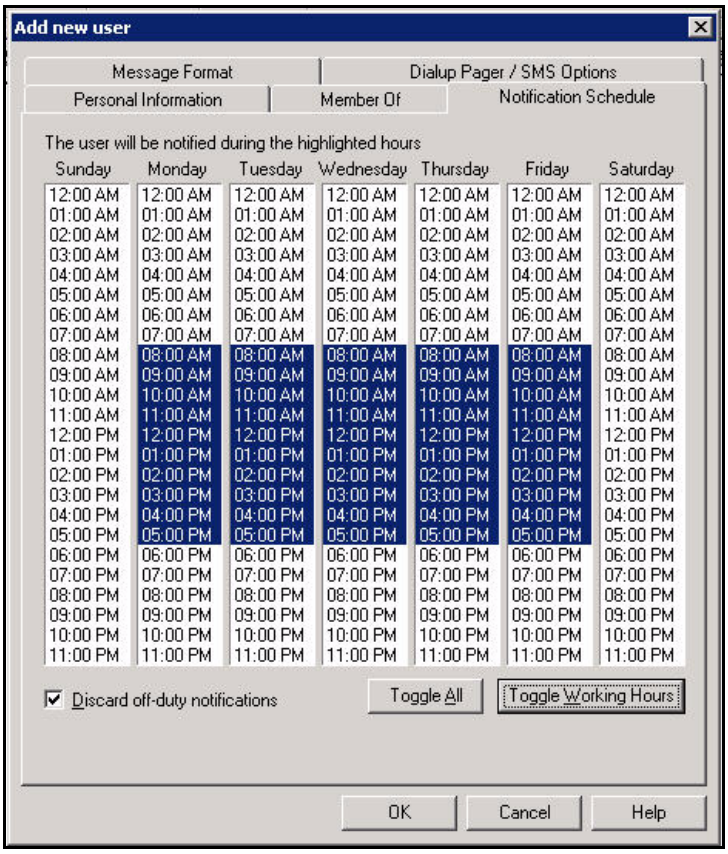


Figure 14: Add New User: Notification Schedule tab

Message Format

nFX Log One's **Message Format** feature allows you to restrict the amount of data being sent to e-mail addresses or pagers as some pagers restrict the amount of data they can accept. If too much data is sent over a page, the sent information will be truncated.

1. In either the **Add new user** or **User Properties** dialog box, select the tab: **Message Format**.
2. Within the **E-mail**, **Pager**, or **SMS/GSM** sections, uncheck any option you would like to not appear in the email message being sent.

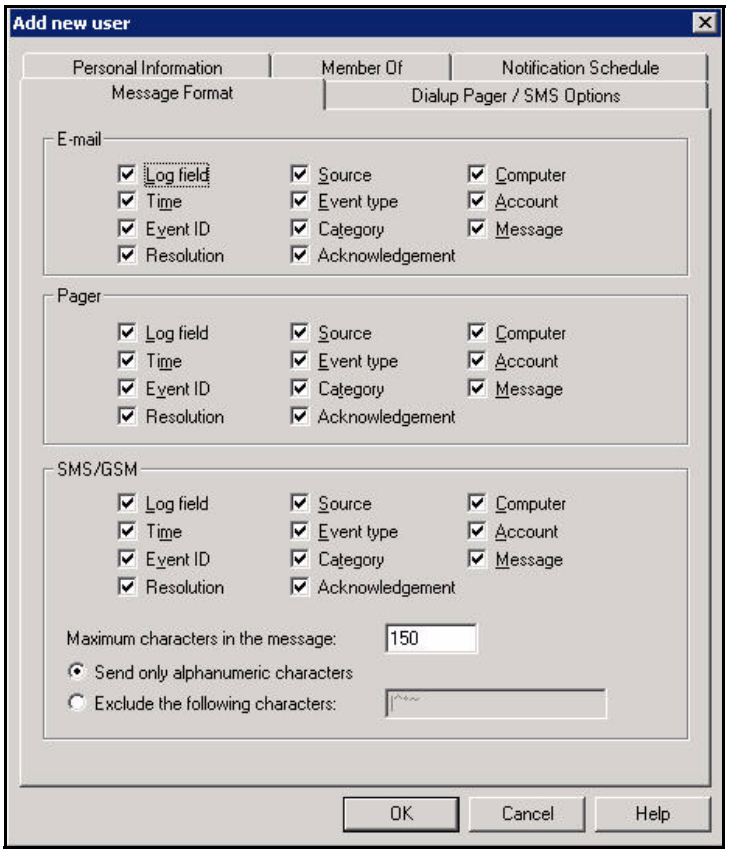


Figure 15: Add new user: Message Format tab

If you choose to use **SMS/GSM** email, you must have an **SMS/GSM Gateway Server** configured. SMS/GSM Gateway Server must be able to convert e-mail messages sent by nFX Log One to SMS/GSM Protocol Messages before sending those messages to the users' mobile phone.

3. Click **OK**.

Important

Some SMS/GSM Gateway Servers do not convert special characters located in the text of the Windows Event message (i.e., <> characters). Therefore the SMS/GSM Gateway Server must filter out special characters in order for the message to be sent properly to the user's mobile phone. Enter these characters in the Exclude the Following Characters field located at the bottom of the **Add New User** screen.

Dialup Pager & SMS Options

To locate this the **Dialup Pager / SMS Options** screen:

1. In either the **Add new user** or **User Properties** dialog box, select the tab: **Dialup Pager / SMS Options**.
2. Under **Pager Settings**, select the **Pager Type** used by the user (alphanumeric or numeric only).
3. If you are using **SMS/GSM e-mail**, enter the user's mobile phone number in the **Phone Number** field located under the GMS/SMS Settings section.
   - » nFX Log One places this telephone number in the Subject Line of the e-mail notification message sent to the Gateway Server.

The Gateway Server will then convert the e-mail message to SMS or GSM and send it to the mobile phone number that was included in the Subject Line of the e-mail message.

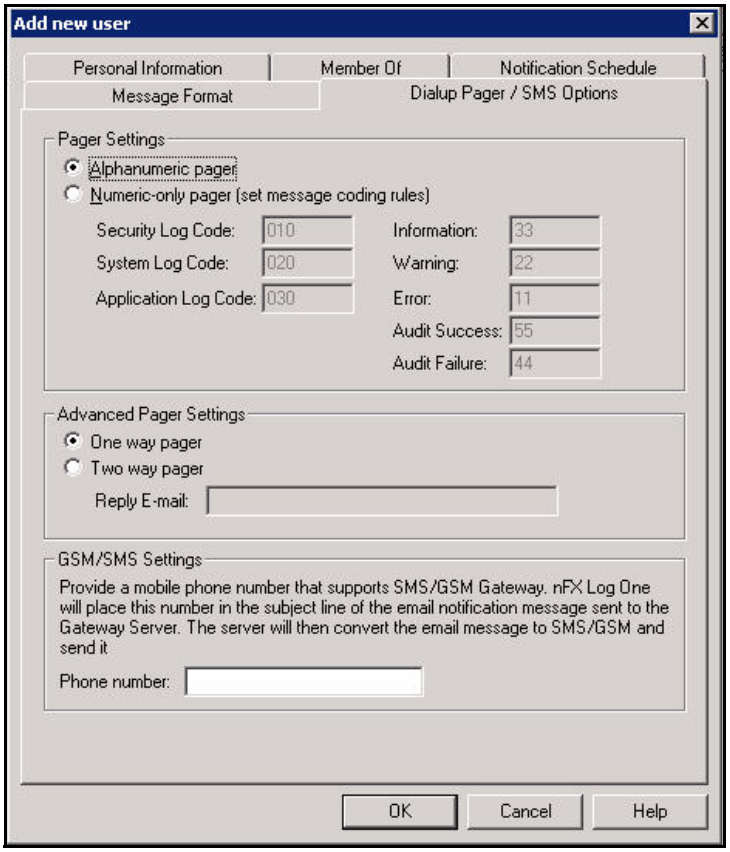


Figure 16: Add New User : Dialup Pager Settings tab

Important

Enabling SMS/GSM e-mail *eliminates* the option to send regular e-mail to the user with this particular profile.

Creating Business Groups

For organizational purposes and to set up **Notification Groups**, you can group **Agent Computers** and **Users** into **Business Groups**. You can also apply **Group Level Privileges** to **Business Groups** or create specific **Business Group Privileges** for *specific* Users.

- The **Enterprise Business Group** is created automatically when you install nFX Log One onto your system.
- The **Enterprise Business Group** cannot be renamed or deleted.
- By default, nFX Log One places all of the computers and new users into the **Enterprise Business Group** including the local nFX Log One Server system.
- A system can only belong to a single Business Group at a time.

The following information will instruct you on how to create a **Business Group**.

1. **Right-click** in the upper left pane of the **Setup** screen.
2. Select ***New > Group***.

» The **Add New Business Group** screen displays.

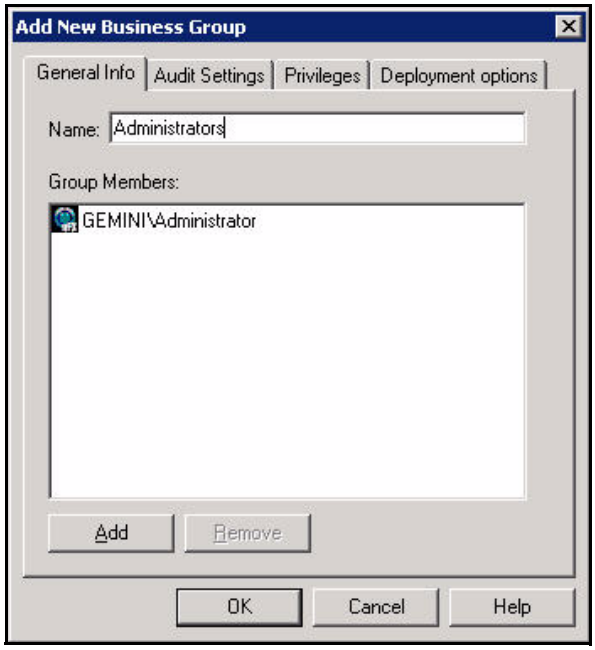


Figure 17: Add New Business Group: General Info tab

General Info Tab

1. From the **General Information** tab, enter a name for the Group you are creating in the **Name** field.
2. Add the names of the users that you would like to include in this Group in the **Group Members** box by clicking the **Add** button. (Conversely, use the **Remove** button to remove **Group Members**).
3. When finished, click the **OK** button.

Business Group Properties

Additional information can be set or changed for Business Groups during or after their creation.

The following sections describes additional information as relates to Business Group Properties. The following tabs are described below:

- Audit Settings
- Privileges
- Deployment Options

These tabs can be located:

- When creating a new Business Group, in the **Add New Business Group** dialog box found by **right-clicking** in the upper left pane of the **Setup** screen and selecting ***New > Group*** or,
- For existing Business Groups, in the **Business Group Properties** dialog box found by **right-clicking** the Business Group name in the upper left pane of the **Setup** screen and selecting **Properties**.

Audit Settings

Audit Settings can be made at either the **Group Level**, which change the settings on all computers in that **Group** or at the **Computer Level**, which only changes audit settings on the selected computer.

Important

Active directory group audit policies will override audit settings configured by nFX Log One.

Privileges

The **Privileges** tab allows you to create settings that apply to specific **Business Groups**. This setting is used to *limit* the privileges of the individual members of a specific Business Group by *restricting* the use of features and configuration screens within nFX Log One.

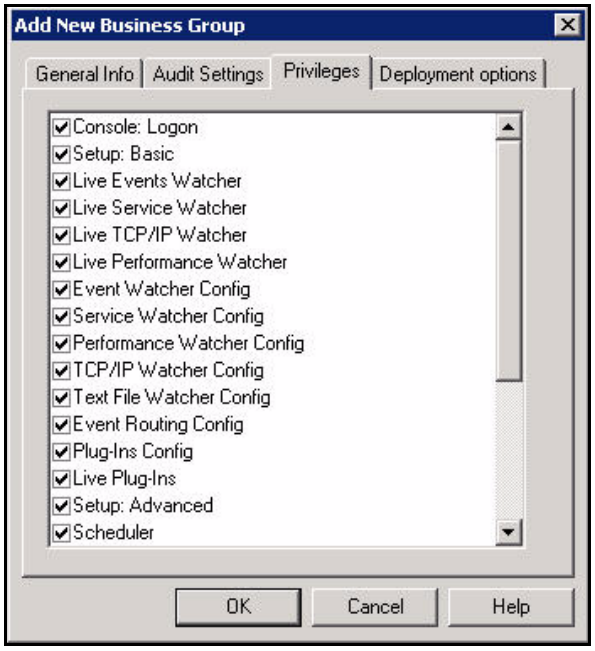


Figure 18: Add New Business Group: Privileges tab

Important

You can create **Business Groups** which contain several different privilege schemes, from loose to strict permissions. For example, you can create a Business Group named *Senior Administrators* and then apply loose permissions to allow extensive mobility throughout nFX Log One. At the same time, you can create a Business Group named *Junior Administrators* and then apply strict permissions to allow very little mobility throughout nFX Log One.

Deployment Options

From the **Deployment options** tab you can configure nFX Log One to use the default **Monitored Systems Group** options to prevent having to enter this information for all new Business Groups added. You can also provide alternate deployment options for new Business Groups to allow deployment and management of computers in other non-trusted domains.

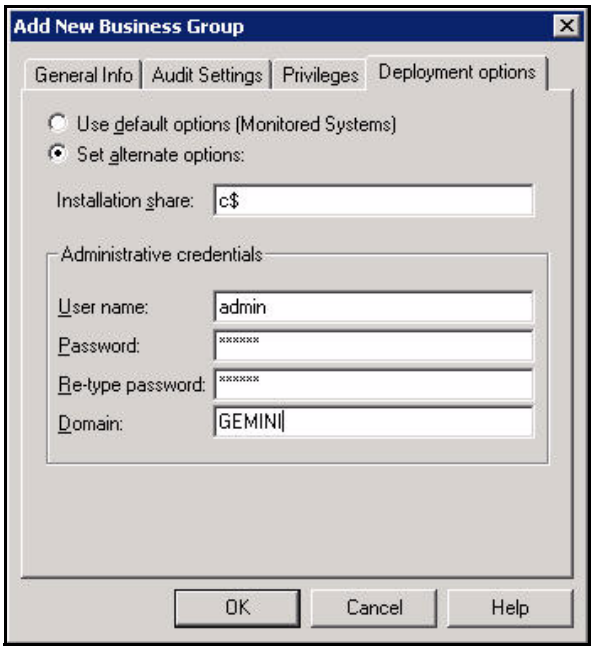


Figure 19: Add New Business Group: Deployment Options tab

Configuring Corrective Actions

You can configure nFX Log One to execute **Visual Basic (VB)** scripts or batch files when certain **Events** are detected from an **Agent** computer or these files can be executed at scheduled times using the **nFX Log One Scheduler** feature. **Corrective Actions** must first be defined in **nFX Log One Setup**.

You can add a **Corrective Action reference file** by following the steps listed below.

1. **Right-click** in the upper left pane of nFX Log One **Setup** screen.
2. Select ***New > Corrective Action***.
3. Locate the Corrective Action **file** by clicking **Browse**.
4. Select the desired Corrective Action **file**.
5. Click **Open** to return to the **Correction Action** dialog box.
6. Enter a **Description** of the Corrective Active **file** (optional).

7. Click **OK**.

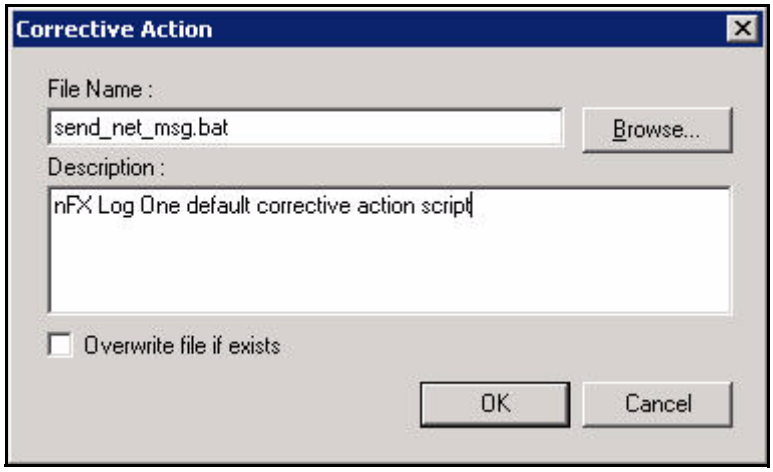


Figure 20: Corrective Action dialog box

Important

The corrective action files will be copied to the nFX Log One database and also can be found in the **c:\Program Files\netForensics\nFX Log One\bin\CorrectiveActions** directory.

Event Routing Configuration

Event Routing Configuration is where you configure nFX Log One to route E-mail, Pager, and SNMP alerts.

To access the **Event Routing Configuration Setup** screen, follow these steps:

1. **Right-click** on **Event Routing Configuration** in the upper left pane of **Setup** screen.
2. Select **Properties**.
   - » A dialog box appears with three tabs: **E-mail**, **Generic Dialup Page**, and **SNMP Traps Generator**.

   Follow the instructions under each of the tab headings listed below.

E-mail Tab

1. From the **E-mail** tab, select the **Enable** checkbox.
2. Enter the **Sender's email address** in the **Sender's E-mail Address** field.
3. Enter the **Sender's name** in the **Sender's Name** field.
4. Enter the **Sender's organization** in the **Sender's Organization** field.
5. Use the drop-down list next to the **E-Mail Format** field to select the e-mail format that you would like to use. Your options are **Text** and **HTML**.
6. Use the **Add** button to enter the IP Address, Port Name or Domain Name, of your SMTP Server. Similarly, use the **Remove** or **Edit** buttons for the **SMTP Servers** respectively.
7. Once you have finished entering all of the necessary information for the **E-mail** tab, highlight your **SMTP Server name** and click the **Test** button to verify communications.

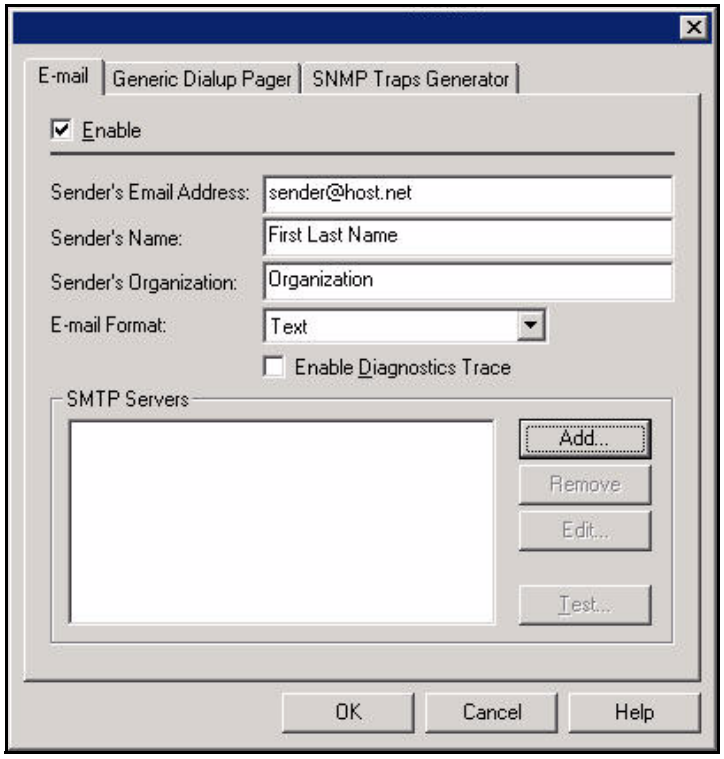


Figure 21: E-mail Tab

Important

An **Enable Diagnostics Trace checkbox** is included so that you can test email functionality through nFX Log One.

Generic Dialup Pager Tab

The **Generic Dialup Pager** tab allows you to send pages using the **TAP protocol**, which requires a separate modem that the nFX Log One Server can access locally.

1. From the **General Dialup Pager** tab, select the **Enable** checkbox.
2. Enter the necessary information for Pager and Modem settings.

Important

You will need to verify communications settings with your Pager service provider.

3. Click the **Test** button to test the pager functionality in nFX Log One.

4. When you have finished entering all of the necessary information in the **General Dialup Pager** tab, click the **OK** button.

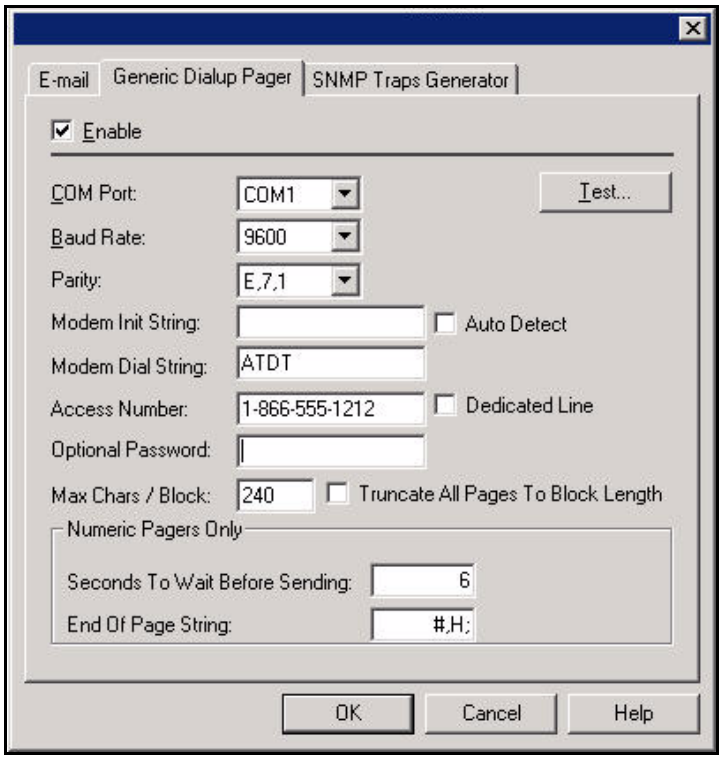


Figure 22: General Dialup Pager tab

SNMP Traps Generator Tab

The **SNMP Traps Generator** tab allows you to tell nFX Log One where to send SNMP traps for real time alerts.

The information entered in the **SNMP Traps Generator** tab allows you to generate SNMP traps (v1 or v2) for any event processed by the **Event Dispatcher Server**. The **MIB** file for **nFX Log One Generated Traps** is located in the **\nFX Log One\MIb** directory. The name of the file is **nFX Log One.mib**. Compile and load this file in your **SNMP Console** to make it aware of the data types used by the **nFX Log One Generated Traps**.

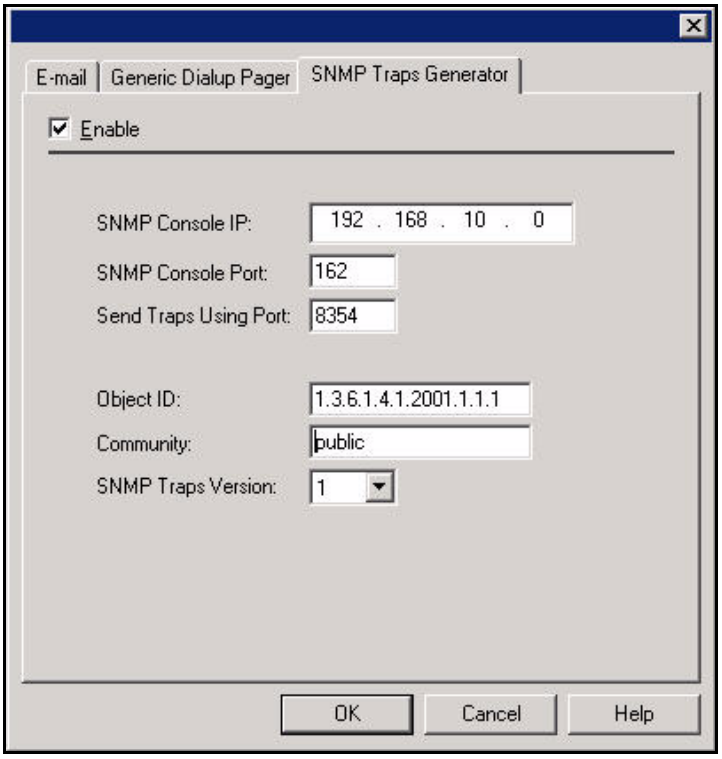


Figure 23: SNMP Traps Generator tab

1. From the **SNMP Traps Generator** tab, select the **Enable** checkbox.
2. Enter the **IP address** of the **SNMP Console** that you are using in the **SNMP Console** field.
3. Enter the **SNMP Console Port** where traps are expected in the **SNMP Console Port** field. By default this Port is **162**.
4. By default, the **Object ID** field is set to **1.3.6.1.4.1.2001.0.1.0. 1.3.6.1.4.1.** 2001 is the Object ID. {Zero (0) is nFX Log One. One (1) is the Dispatcher and 0 is the SNMP Route.} **Note:** If the Object ID conflicts with another Object ID already defined within your enterprise, you can change the Object ID to anything that you want.
5. By default the Community field for the SNMP Community is set to **Public**. You can change it to any other SNMP Community suitable for your enterprise.
6. Enter the **Version Number** of the traps that you want to generate in the **SNMP Version Traps** field. Enter **1** for **SNMP V1** traps and **2** for **SNMP V2** traps. SNMP V1 is the default.
7. When you have finished entering all of the necessary information in the **SNMP Traps Generator** tab, click the **OK** button.

Log Management and Archiving

nFX Log One's **Log Management** features provide end-to-end log management functions for all log types such as Windows event logs, syslogs, supported application logs, as well as logs and files of binary and proprietary formats. Log management functionality is available on all systems running an nFX Log One agent.

nFX Log One's **Log Management** features include: log signing, compression, encryption, archiving using secure transport, log retrieval, and integrity validation of the log files.

The **log signing** feature allows all log files to be digitally signed using SHA (Secure Hash Algorithm). This hash is immediately sent back to the nFX Log One Server and stored in the nFX Log One SQL database for future log file validation. By default nFX Log One will compress & encrypt the files immediately after the hash using AES (Advanced Encryption Standard) as recommended by NIST (National Institute of Standards Technology). The files are then sent to the designated Log Management archive system. nFX Log One must be running on the system if designated as the archive machine. The log validation feature which is run from the netForensics Reporting Web Console (see "Validating and Viewing Encrypted Logs" on page 40) checks the authenticity of all aggregated logs files across the enterprise by verifying the digital signature.

Log Archiving

Log Archiving is an important part of **Log Management**. With nFX Log One. You can consolidate or archive collected log files once a day from all agents to a single **nFX Log One Archive System**.

The steps below provide instructions on how to setup **Log Archiving**:

1. From the **nFX Log One Console** toolbar select ***Tools > Archive Logs***.
   - » The **Archive Logs - Configuration Settings** dialog box displays.

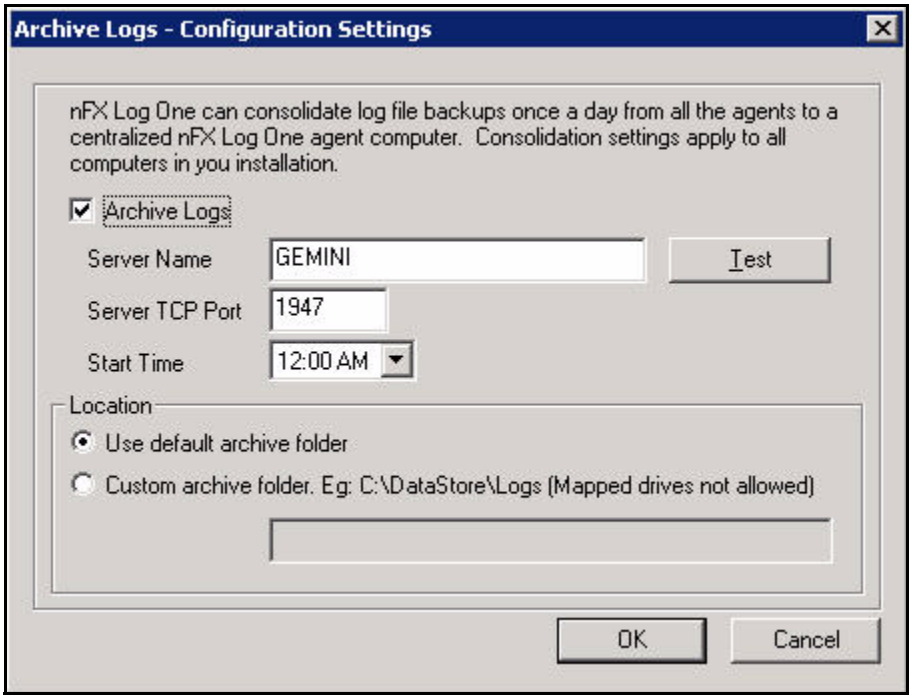


Figure 24: Archive Logs - Configuration Settings dialog box

2. Check the **Archive Logs** checkbox.
3. Provide the following **Configuration Settings**:
   - **Server Name** - machine name where an nFX Log One Agent has been deployed
   - **Server TCP Port** - default is 1947
   - **Start Time** - time when the backups should start
   - **Location** - directory where the logs will be saved. This drive must be a logical drive (no mapped drives) located on the selected machine or IP address. If left blank, the default location is: **`c:\Program Files\netForensics\nFX Log One\Data\Backup`**.

4. When finished entering data, click **OK**.

Important

Archive Log Configuration Settings apply to all computers in your installation.

Event Log Management

The **Event Log Management** feature is used to define event log backups and management settings of all Windows Event Logs being managed by nFX Log One.

Important

Event Log Management is set to **Windows Event Log Management** by default. nFX Log One will change the retention setting to '**Overwrite as needed**' if not already set otherwise no other changes are made to **Windows Event Viewer** settings.

If **nFX Log One Event Log Management** is selected, the nFX Log One Agent will immediately change the retention settings of the selected agent machines to '**Do Not Overwrite**'. The **nFX Log One Agent** will automatically backup, sign, compress, encrypt, and reset each Event Viewer log when the maximum log size setting has been reached. You can alternatively set nFX Log One to also backup by time forcing a backup of all **Event Viewer** logs based on a set number of days.

'To access the **Event Log Management** utility, follow the steps below:

1. From the **nFX Log One Console** toolbar, select ***Tools > Event Log Management***.
   - » The **Event Log Management** dialog box displays.

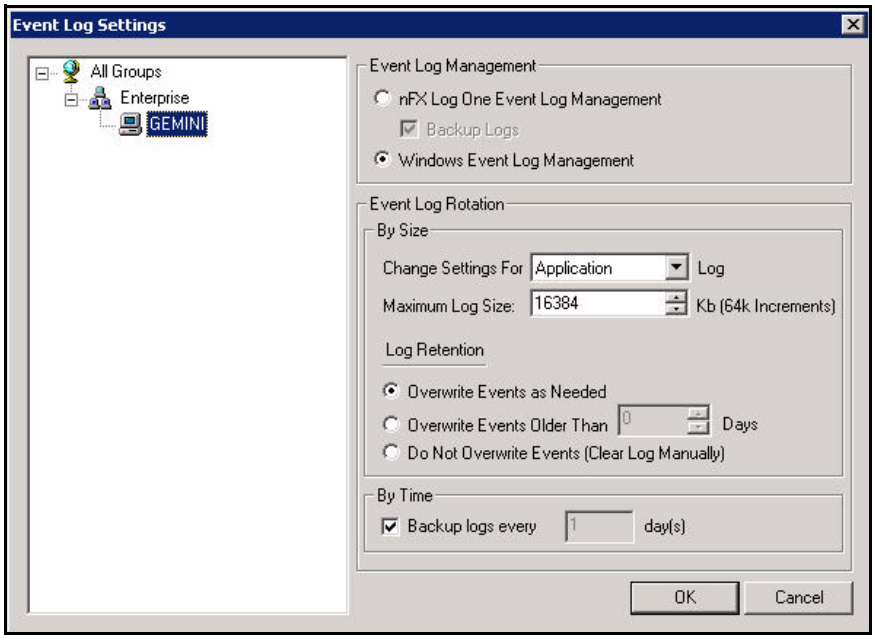


Figure 25: Event Log Settings dialog box

   - » The left pane of the window lists the **Business Groups** and **Computers** in a tree format.
2. **Highlight** the desired **Computer** or **Business Group** to be configured.

3. In the **Event Log Management** section, select the radio button for either **nFX Log One Event Log Management** or **Windows Event Log Management**.

Important

If **nFX Log One Event Log Management** is selected, nFX Log One will manage the logs and automatically reset and backup the event logs when the user-defined criteria provided is reached. If **Windows Event Log Management** is checked, you can use these configuration options to define a central policy for Windows to use in handling **Event Log Management**. If the **Compress Backups** box is checked the logs will be compressed before consolidating.

Important

If you select **nFX Log One Event Log Management**, you have the option of having nFX Log One consolidate the Event Log backups to the specified server once a day. See *"Log Archiving" on page 37* for more information.

4. In the **Event Log Rotation** section, select the drop-down box in the **Change Settings For**, to configure any of your Windows Event logs.
5. In the **Maximum Log Size** field, enter the anticipated maximum size for that log. Make sure to set the correct log size for each log. This field can be incremented by using the up/down arrows. The size can be adjusted by 64K increments.

Important

It is important to understand when **nFX Log One's Event Log Management** will make backups of *Window Event Viewer* logs. nFX Log One will monitor the size of the log file on each nFX Log One Agent computer. When the maximum log size (as defined above) is reached, the nFX Log One Agent creates a copy of the Event Log on the nFX Log One Agent computer. This copy will NOT be forwarded to the nFX Log One Server until the time set archive time has been reached. If the log takes 3 days to reach the maximum size, then no copies of the log will be sent to the nFX Log One server until the designated time on the third day unless the By Time setting has been satisfied. The logs are archived to the **`Program Files\netForensics\nFX Log One\Data\Backups`** folder by default unless specified in the ***Tools > Archive Logs*** screen.

6. When done, click **OK**.

Syslog Management

The **Syslog Management** feature (see "SysLog Watcher" on page 58) provides log management and archiving functionality of all collected **SysLog Watcher** log files from configured devices. i.e.; routers, switches, firewalls, UNIX, AIX and Linux systems.

The default folder for the syslog raw format log files is:
`C:\Program Files\netForensics\nFX Log One\bin\Agent_Home\Repository`

If the agent is setup to manage logs (see "Log Management and Archiving" on page 36) on the Syslog receiver system, the log files will be signed, encrypted, compressed and archived by default to the **Log Management Archive** system. There will be a folder with the device name located in this designated archive folder containing all archived Syslogs.

Third Party Log Management

The **Third Party Log Management Sink** folder feature provides basic log management functionality for logs that are not supported by the nFX Log One Agent. A third party application or a custom batch file can be configured to move or copy these log files to the **`C:\Program Files\netForensics\nFX Log One\Sink`** folder.

If the agent is setup to manage logs (see "Log Management and Archiving" on page 36) on the agent machine where the third party log files will be copied to, the log files will be signed, encrypted, compressed and archived by default to the **Log Management Archive** system in a folder called **Third Party Logs**.

nFX Log One will queue up all of the files placed in the **sink directory** until the designated archive time, then move them to the archive location and validate them just as it would with the logs it supports.

Validating and Viewing Encrypted Logs

You must access the **Log Validation** web page of the **netForensics Web Console** to validate, decrypt, and view archived log files.

To access the Log Validation web page, follow these steps:

1. There are two ways to access the **netForensics Web Console's Log Validation** web page.
   a. By clicking on the **Console** button at the top of the nFX Log One Console
   b. From the **Windows Start** Button on the system where netForensics Reporting has been installed. Select ***All Programs > netForensics > Reporting Admin> Web Console***.
2. From the menu in the left pane, select **Log Management**.
   » The **Log Management Operations** screen displays.

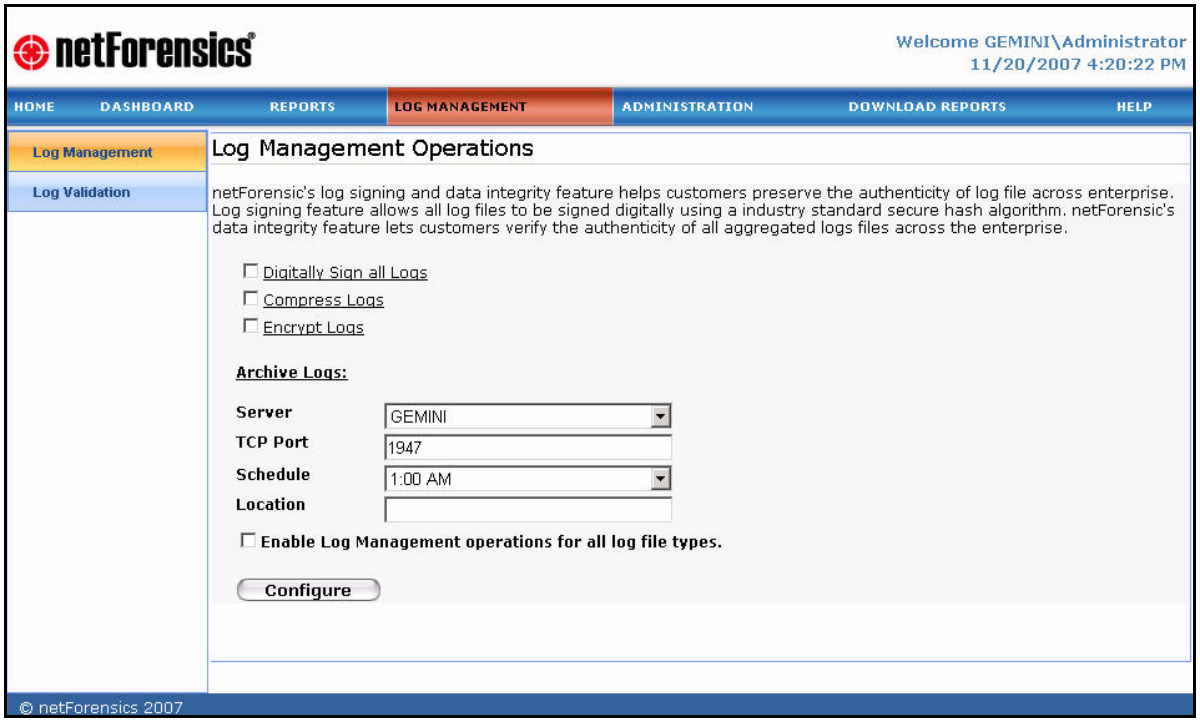


Figure 26: Log Management Operations screen

3. Select the **Log Validation** link on the left menu pane.

» The **Log Validation** screen displays.

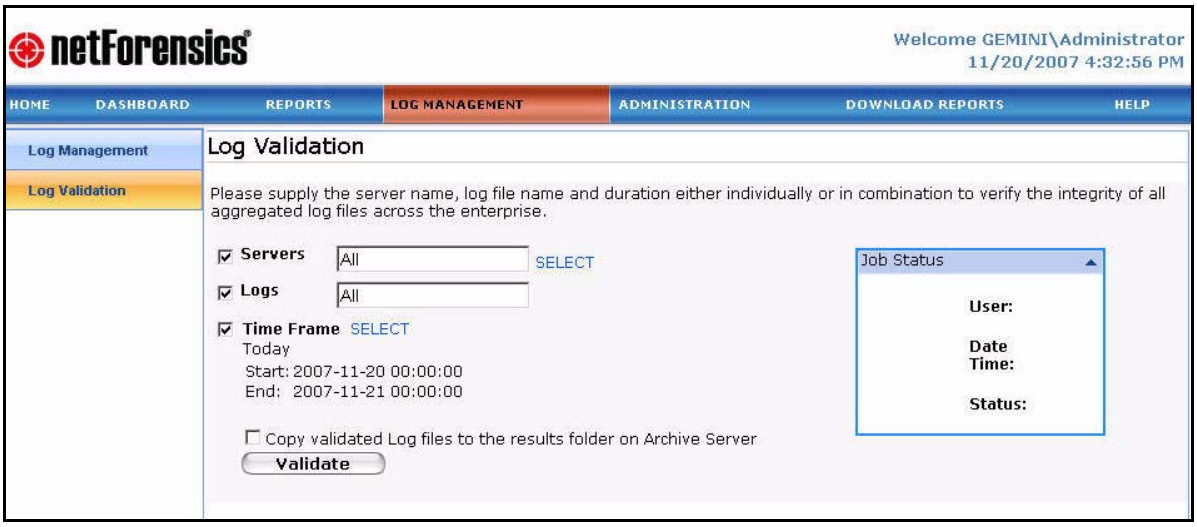


Figure 27: The Log Validation screen

4. In the **Log Validation** section, select the **Server** to be validated.
5. Select the Logs to be validated. Locate the log file from the archive folder that you are validating or making a copy for viewing with extension and copy into the Logs field.

Important

You can alternatively add the log file name and uncheck server and time frame.

6. Check the '**Copy validated Log files**' check box to make a decrypted copy for viewing.
7. Click **Validate**.

» The **Status** indicator should change to '**Processing**'.

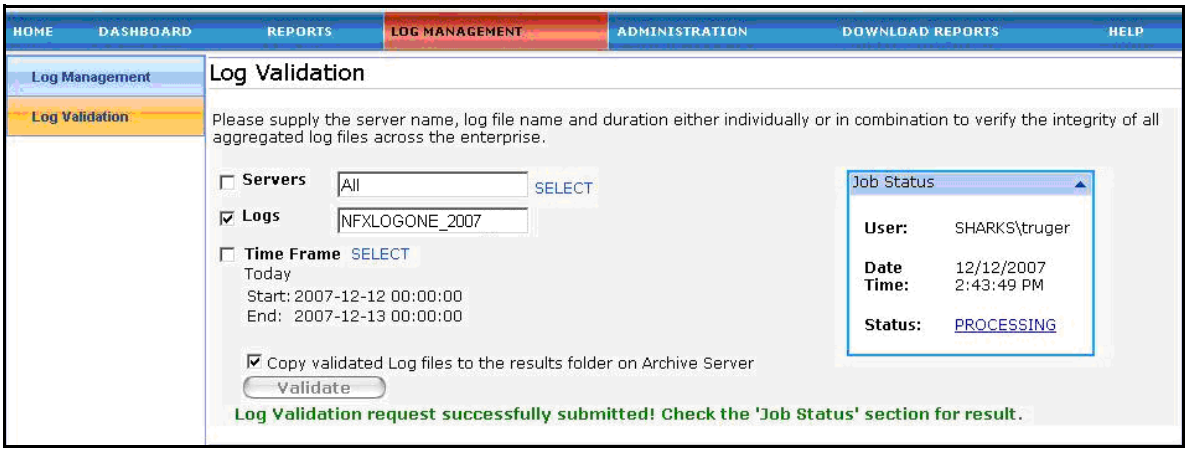


Figure 28: Log Validation Status Message

Important

Decrypting files and making a copy for viewing purposes takes about 2-3 minutes per file so it is highly recommended to be selective with a specific file or names (separated by comma) when making decrypted copies along with validating files. Locate the file in the archive folder and copy the full file name with extension and paste into the Logs field.

8. Click the **Refresh** button from the web console to update the Status indicator.



Figure 29: Log Validation - Completed Status

Important

The **Job Status** section displays the status of the validation job. Because of the default agent polling time, it takes a minimum of two (2) minutes for the status to be updated. Once the validation job is complete, the **+** automatically refreshes.

Warning

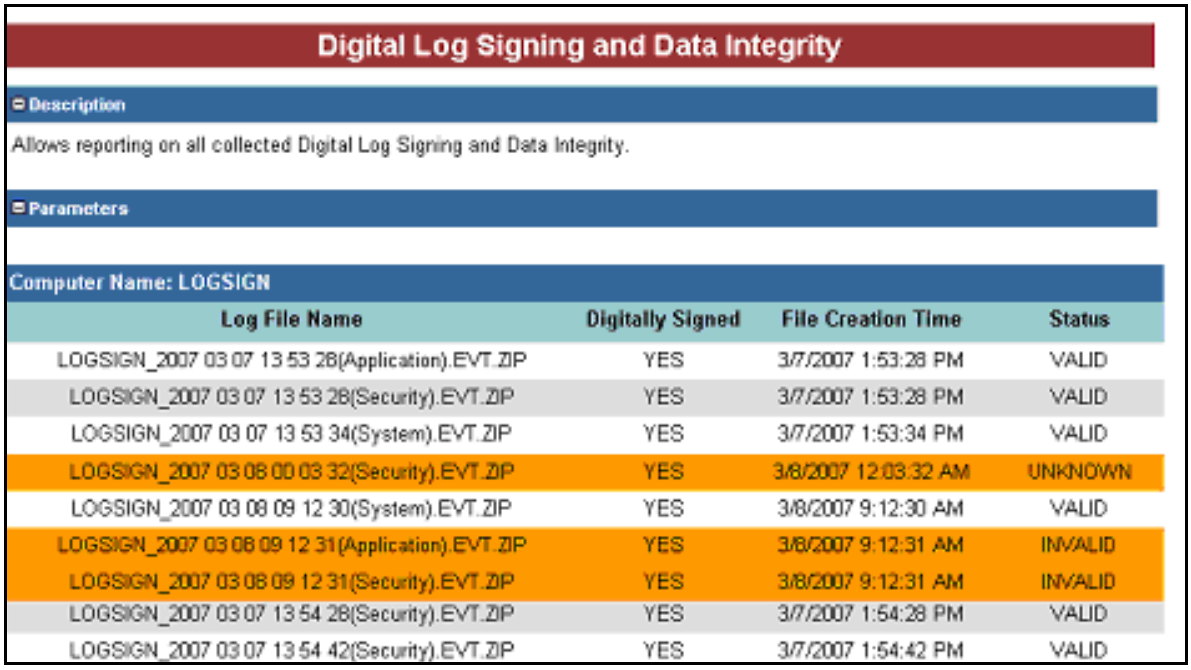
Do not select the **F5** key or the Internet Explorer **Refresh** button as this will re-submit the validation job.

To view the report on integrity of the log files, follow the steps below:

1. In the **Job Status** section, select the Processing or **Completed** Status link.
2. The **Digital Log Signing** and **Data Integrity** report displays in a new window.

Important

Logs that fail the data integrity check have a status of **Invalid** and are highlighted in **orange** text.



Digital Log Signing and Data Integrity

Description

Allows reporting on all collected Digital Log Signing and Data Integrity.

Parameters

Computer Name: LOGSIGN

Log File Name	Digitally Signed	File Creation Time	Status
LOGSIGN_2007 03 07 13 53 28(Application).EVT.ZIP	YES	3/7/2007 1:53:28 PM	VALID
LOGSIGN_2007 03 07 13 53 28(Security).EVT.ZIP	YES	3/7/2007 1:53:28 PM	VALID
LOGSIGN_2007 03 07 13 53 34(System).EVT.ZIP	YES	3/7/2007 1:53:34 PM	VALID
LOGSIGN_2007 03 08 00 03 32(Security).EVT.ZIP	YES	3/8/2007 12:03:32 AM	UNKNOWN
LOGSIGN_2007 03 08 09 12 30(System).EVT.ZIP	YES	3/8/2007 9:12:30 AM	VALID
LOGSIGN_2007 03 08 09 12 31(Application).EVT.ZIP	YES	3/8/2007 9:12:31 AM	INVALID
LOGSIGN_2007 03 08 09 12 31(Security).EVT.ZIP	YES	3/8/2007 9:12:31 AM	INVALID
LOGSIGN_2007 03 07 13 54 28(Security).EVT.ZIP	YES	3/7/2007 1:54:28 PM	VALID
LOGSIGN_2007 03 07 13 54 42(Security).EVT.ZIP	YES	3/7/2007 1:54:42 PM	VALID

Figure 30: Digital Log Signing and Data Integrity Report

Additional **Log Data Integrity** reports are available and can be accessed using the **netForensics Web Console**. You can access these reports through the following menu path: ***netForensics Reporting > Security and Auditing > Log Data Integrity*** folder. Available options are:

- Last Log Validation Results
- Log Archival History
- Log Validation Job History

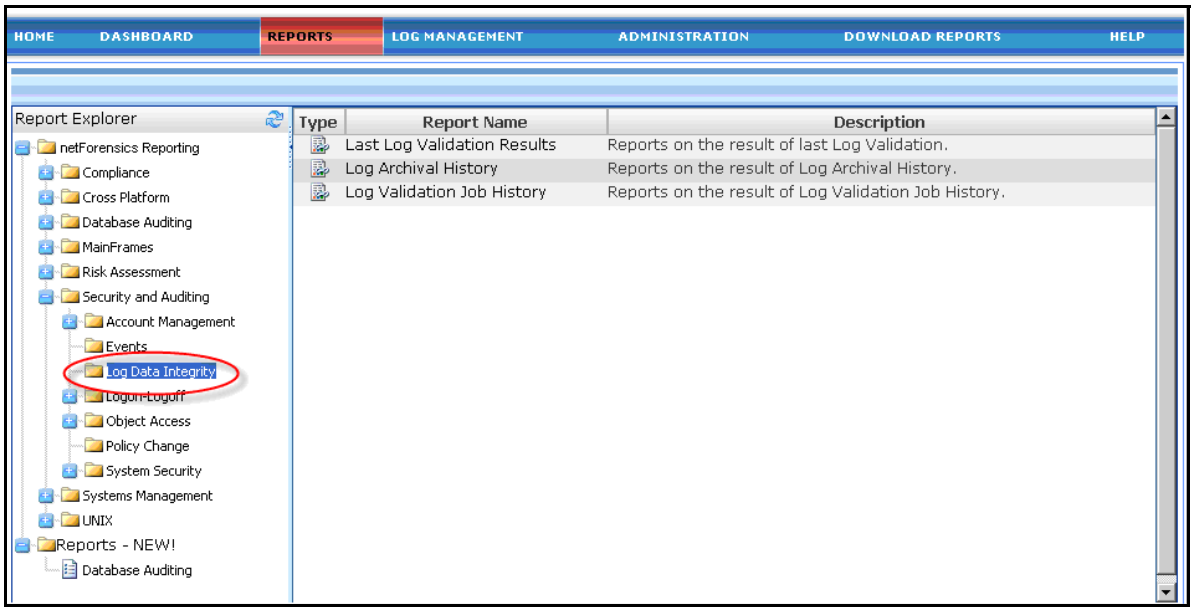


Figure 31: Log Signing & Data Integrity Reports

Log Management Configurations from Web Console

To access nFX Log One Log Management, follow the steps below:

1. From the **Windows Start** Button, select ***All Programs > netForensics > Web Console***.
   - » The **Web Console** screen displays.
2. From the left menu choose ***Tools > Log Management***.
   - » The **Log Management Operations** screen displays.

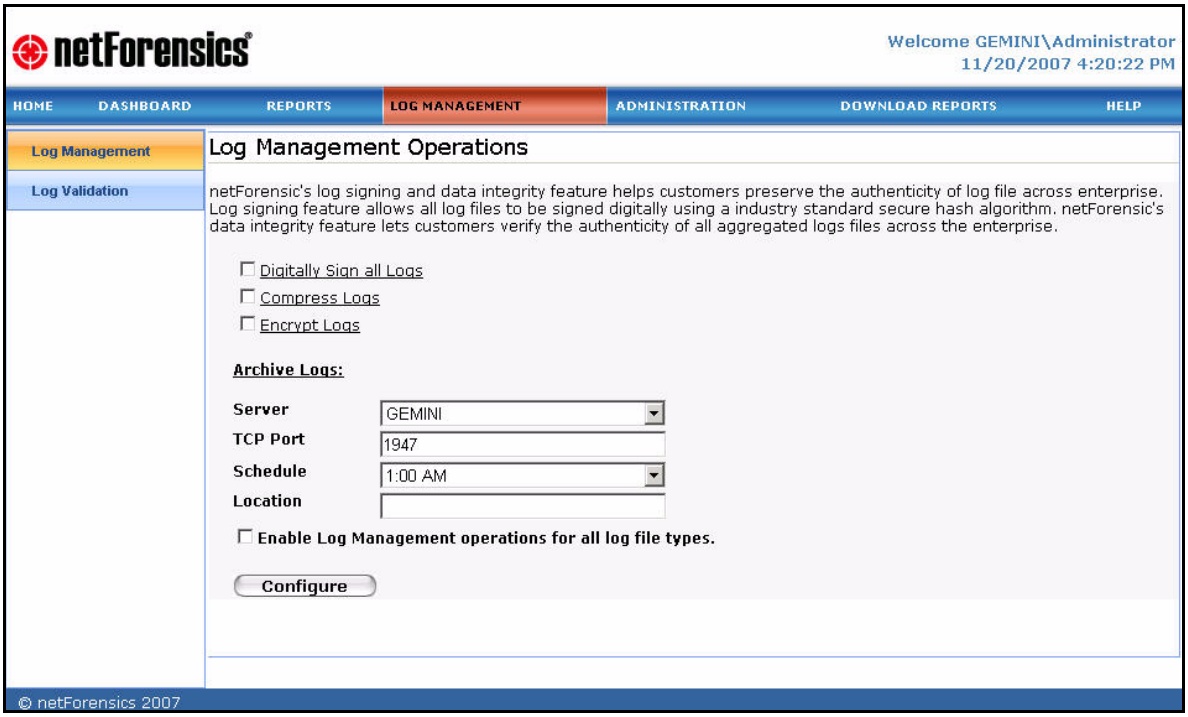


Figure 32: Log Management Operations screen

Event Watcher

In this section you will learn about nFX Log One **Event Watcher**, how it uses rules and how you can create and apply rules. You will also learn about the functions and configuration of nFX Log One Event Watcher and how to view captured events in real time. This section also covers the following topics:

- Importing and Exporting Event Watcher Templates
- Changing the Default Rule Setting

nFX Log One consolidates all **Windows NT/2000/2003/XP Events** from all systems running the nFX Log One **Agent software** onto one manageable console. This viewing area is the **nFX Log One Console Live Events Watcher**. In addition to containing all Windows events, the **Live Events Watcher** contains all events generated by nFX Log One.

The **Live Events Watcher** will only show Events stipulated in the **Event Watcher Rule Set**. By default, nFX Log One is shipped with over 200 rules. These rules are update and made available to customers quarterly.

Important



To condense this information, you can *apply filters* to eliminate unimportant events and apply alerts to alert users on critical events. nFX Log One refers to these events as **Event Watcher Rules** and are designed to help control the amount of traffic being sent from the nFX Log One Agents to the **nFX Log One Management Console**, the urgency applied to the events being sent, as well as the forwarding of notifications to the desired destinations.

Using Rules in Event Watcher

Event Watcher Rules are listed in prioritized order, with the **All Groups** rules container assuming a higher priority than **nFX Log One Business Groups** including the **Enterprise Group**. When a new event is generated on an nFX Log One Agent computer, it is compared to each rule in the **All Groups** list first continuing through rules listed in other **Business Groups**.

When an event is found to match a rule, the **nFX Log One Agent** executes any action specified within that rule. The Event is then either ignored or forwarded along to the nFX Log One Server.

Important



Each nFX Log One Agent *checks* the nFX Log One Agent Server for updates to its *active* Rule Set once per minute.

At the bottom of all **Rule Sets** lies the **Default Event Watcher Rule**. It is highly recommended that you configure the **Default Event Watcher Rule** to ignore (or not forward) these events to the nFX Log One Server. By default, this setting is configured to ignore all events that do not match a rule.

Viewing Live Events in the nFX Log One Console

The Live Event Watcher allows you to consolidate events collected from all **Agent** computers into one viewing screen.

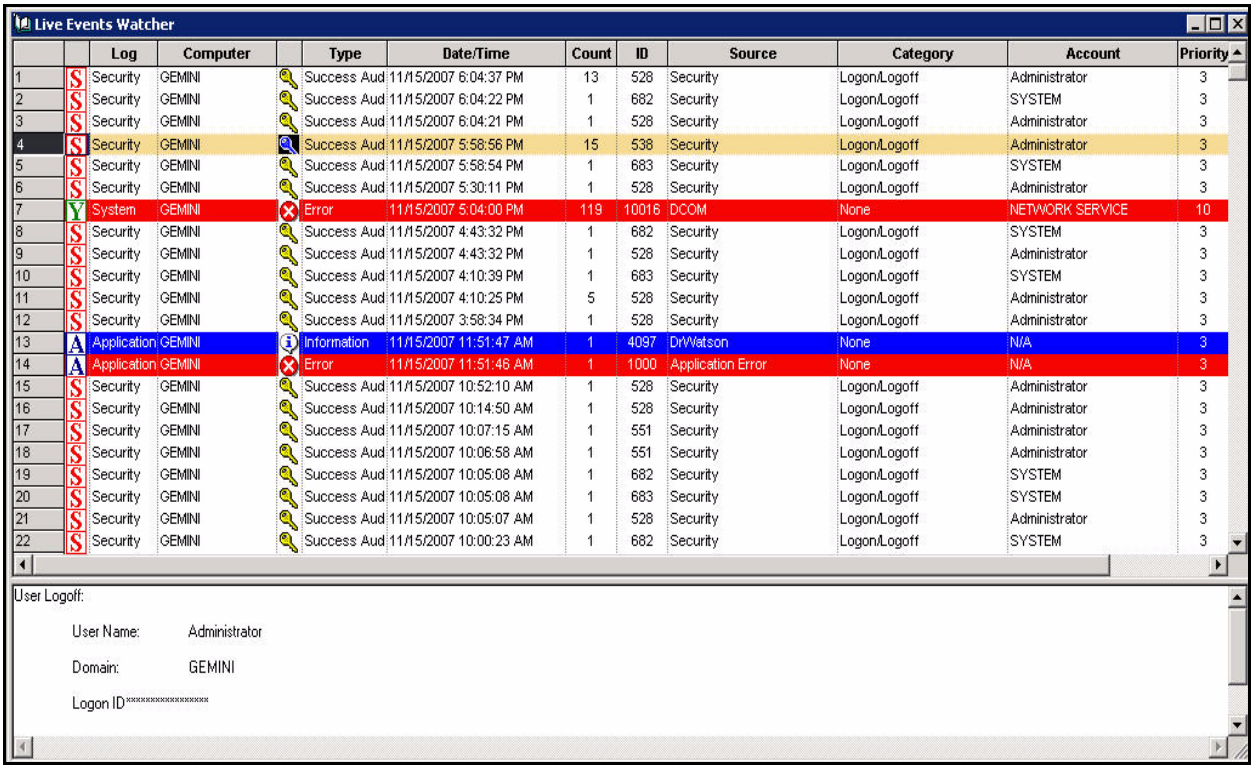


Figure 33: Live Events Watcher screen

The *at-a-glance information* provided in the top portion of the Live Events Watcher screen is displayed in columns. Information regarding each column is listed in the following table.

Column Name	Column Description
Log	The **Log** columns provide you with information about which Log the Event was generated from.
Computer	The **Computer** column represents the computer where the Log was generated.
Type	The **Type** column represents the type of Event that was generated from the computer.
Date/Time	The **Date/Time** column represents the Date and Time that the Log was generated.
Count	The **Count** column represents the number of times the same exact Event Message was generated from one computer.
ID	The **ID** column provides you with the ID number assigned to the nFX Log One Log Entry.
Source	The **Source** column represents the Application associated with the Log Entry.
Category	The **Category** column represents the Application Component generating the Log Entry.

Column Name	Column Description
Account	The **Account** column represents the User Account referenced by the Log Entry.
Priority	The **Priority** column represents the priority of the Log Entry. The column is based on a scale from 1 to 10, with 10 being the least important type of Log Entry.

Table 3: Columns in the Live Events Watcher screen

Important

Right-clicking on a column name provides you with options for adding or deleting columns from your live view, as well as sorting column information in ascending or descending order. You can also adjust the column size by using your mouse to drag the column width markers to the right or left.

Customizing the Live Event Watcher

nFX Log One allows you to customize the Live Event Watcher.

1. From the menu, select ***View > Preferences***.
   - » The **Preferences** screen displays.

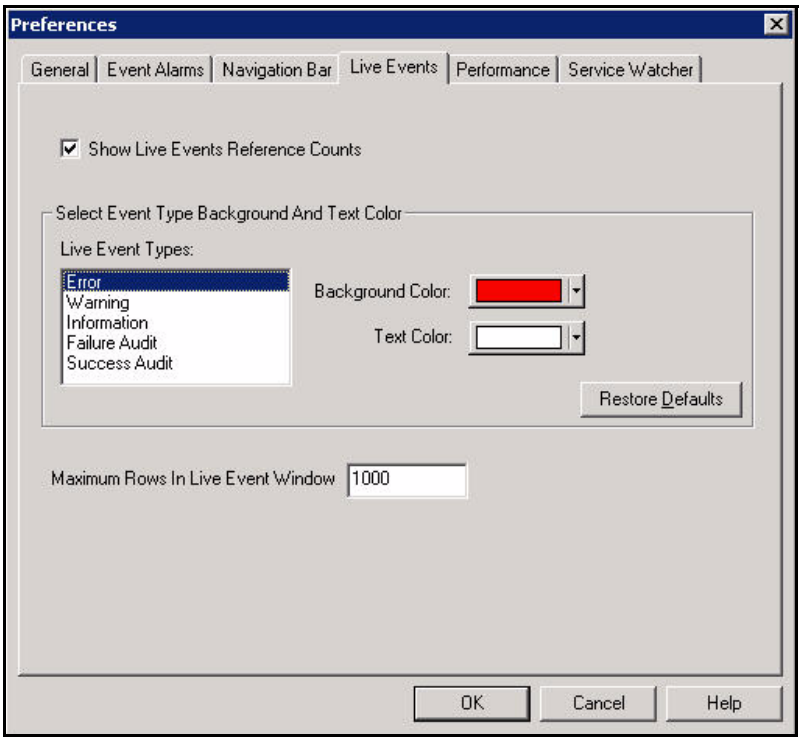


Figure 34: Preferences dialog: Live Events tab

2. Select the **Live Events** tab.
3. If you want to view each individual occurrence of an event, **uncheck** the **Show Live Events Reference Counts** checkbox. If you do not want to view each individual occurrence, **check** the **Show Live Events Reference Counts** checkbox.
4. To change the **background color** of an **Event Type**:

a. Select the **Event Type** (i.e., Error, Warning, etc.) that you would like to assign a new background color to from the Live Event Types box.

b. Once you have selected the **Event Type**, select the **Background Color** for that event by using the drop-down menu located next to the **Background Color** box to select a color.

5. To change the **text color** of an **Event Type**:

   a. Select the **Event Type** (i.e., Error, Warning, etc.) that you would like to assign a new text color to from the Live Event Types box.

   b. Once you have selected the **Event Type**, select the **Text Color** for that event by using the drop-down menu located next to the **Text Color** box to select a color.

6. You can change the maximum number of rows displayed on the Live Event screen by entering a number in the **Maximum Rows In Live Event Window** field. Keep in mind that once this number is exceeded the old events will be truncated. The default number of events is 1,000. The maximum number of events is 10,000.

Event Watcher Rules

nFX Log One ships with a comprehensive set of predefined standard rules to assist you in tracking internal security and auditing -- right out of the box and upon initial installation. You can keep, modify, or delete these rules. nFX Log One provides you with five types of **Event Watcher Filter rules**, including:

- An Event Watcher Rule created from a **Live Event**
- A **Custom** Event Watcher Rule
- An Event Watcher Rule created from an included standard **NT Event** database
- An Event Watcher Rule created from an **Event Report**
- An Event Watcher Rule imported from an **Application template**

Creating an Event Watcher Rule from a Live Event

The easiest way to create an **Event Rule** is to follow the steps listed below:

1. From the **nFX Log One Console**, select ***Go >Live Events Watcher***.

   » The **Live Events Watcher** screen displays.

2. **Right-click** on the **Event** that you want to create a **Rule** for.

3. Select **Create Event Watcher Rule from Event** from the right-click menu options.

4. Select a **Group** where to create the Rule.

5. Click **OK**.

» The **Event Watcher Config** screen displays.

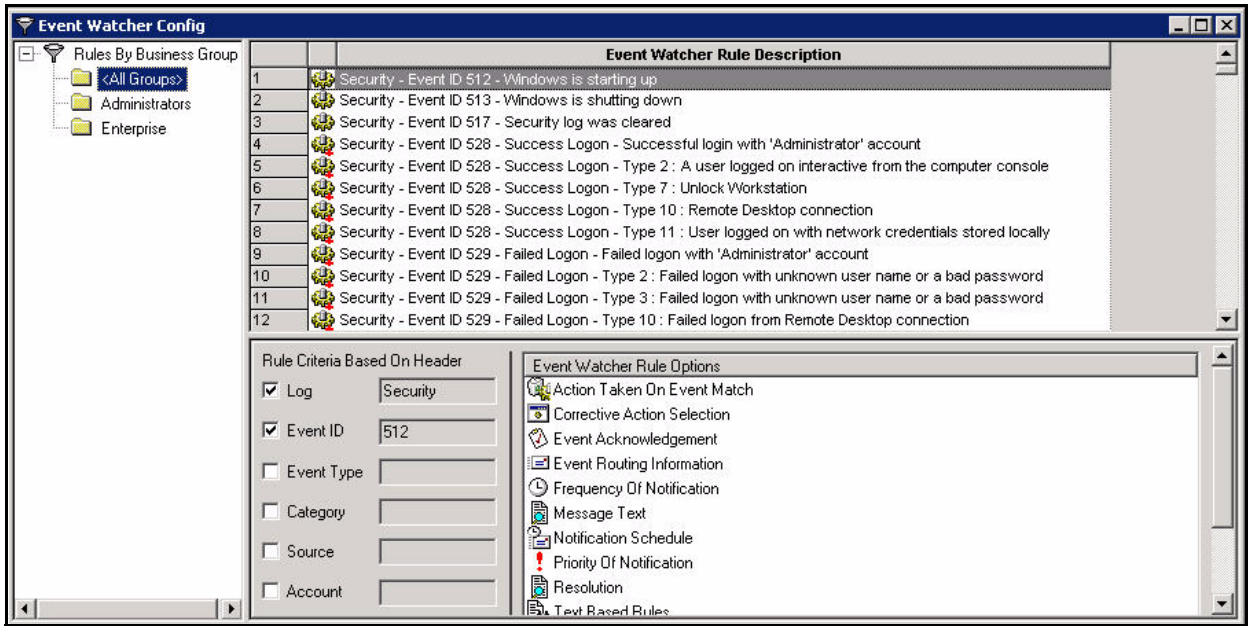


Figure 35: Event Watcher Config screen

The Event Watcher Config screen is divided into four sections. Each section is described below.

- The **Event Watcher Rule Description** section lists the rules already configured for the **Business Group** that is highlighted in the **Rules By Business Group** section.
- The **Rules By Business Group** section lists the **Business Groups** created from nFX Log One **Setup**. It also lists a default group called **<All Groups>** to be used when you want to apply an Event Watcher Rule to all Business Groups.
- The **Rule Criteria Based on Header** section lists the options that must be present in an Event for the actions located in the **Event Watcher Rule Options** section to occur. The criteria can be as general or as specific as you choose.
- The **Event Watcher Rule Options** section is where you determine what actions nFX Log One will do when the options in the **Rule Criteria Based on Header** section are met by an Event.

Using the Event Watcher Rule Description Pane

The **Event Watcher Rule Description** pane is where the nFX Log One **Administrator** spends the most time. Therefore, it is very important that you implement a descriptive naming convention to your rules and be very careful about of how you position those rules.

Important



It is recommended that you *initial* Custom Rules and move them to the top of the **All Groups** Rules list.

In nFX Log One, you can custom define Event Watcher Rules for certain types of Windows Servers, which allows you to push *very* specific rules to these Servers. You can do this by moving rules to *certain* **Business Groups**.

In order to accomplish this task, nFX Log One *compares* **New Events** to the **Event Watcher Rules** listed in the **All Groups** folder, and uses a hierarchical format for filtering these events. Once an Event Watcher Rule has been matched with a Windows Event, nFX Log One will not look at any rules listed below the present match.

Using the Event Watcher Rule Functions

From the **Event Watcher Rule Description** screen, you can perform several key functions, including:

- Renaming an **Event Watcher Rule**
- Moving or copying an **Event Watcher Rule** to a **Business Group**
- Moving an **Event Watcher Rule** up or down within **Rule** list
- Moving an **Event Watcher Rule** to the top of **Event Watcher Rule** list

The following section will instruct you on how to complete these tasks.

Follow the steps below to rename an Event Watcher Rule:

1. From the **Event Watcher Rule Description** screen, **right-click** on the **Event Watcher Rule** that you would like to rename.
2. Select the **Rename Event Watcher Rule** option.
3. Rename the Rule and click the **OK** button.

Follow the steps below to move or copy an Event Watcher Rule to a Business Group:

1. From the **Event Watcher Rule Description** screen, **right-click** on the **Event Watcher Rule** that you want to **move** or **copy** to a Business Group.
2. Select the **Copy to Business Group(s)** or **Move to Business Group(s)** option.
3. Select the **Business Group(s)** and click the **OK** button.

Follow the steps below to move an Event Watcher Rule up or down within the Event Watcher Rule Description list.

1. From the **Event Watcher Rule Description** screen, **right-click** on the **Event Watcher Rule** that you want to move **up** or **down** within the Event Watcher Rule description list.
2. Click on the **Number** of the corresponding Rule (row) that you want to move.
3. **Hold** the left mouse button down on that Rule.
4. **Drag and Drop** the Rule to the new location.

Follow the steps below to move an Event Watcher Rule to the top of the Event Watcher Rule Description list.

1. From the **Event Watcher Rule Description** screen, **right-click** on the **Event Watcher Rule** that you want to move to the top of the Event Watcher Rule description list.
2. **Right-click** on the Rule.
3. Select **Move Event Watcher Rule to the Top**.

Rule Criteria Based on Header

The **Rule Criteria Based on Header** pane check boxes are what determine if a Windows Event matches one of nFX Log One's Event Watcher Rules. In order to configure a Rule to be more generic in matching Event types, you can deselect any **Rule Criteria Based on Header** Information checkboxes listed.

You can also add other criteria using the **Text Based Rules** option.

1. From the **Event Watcher Rule Description** screen, in the lower right window pane, select **Text Based Rules**.
2. Now you can add certain *keywords* (in the lower left pane) to allow nFX Log One to look for specific keywords in the **Message Text** of the Event that matches the Rule. Use the **Add** button to add keyword and the **Remove** button to remove keywords.

3. When finished, click **OK**.

Important

Multiple keywords are allowed, however all keywords must be present in the Message Text of the Event.

Event Watcher Rule Options

The **Event Watcher Rule Options** pane contains **10 configurable options** for each Rule. They are:

1. Action Taken on Event Match Option
2. Corrective Action Selection Option
3. Event Acknowledgment Option
4. Event Routing Information Option
5. Frequency of Notification Option
6. Message Text Option
7. Notification Schedule Option
8. Priority of Notification Option
9. Resolution Option
10. Text Based Rules Option

Important

You can reach the **Configuration Parameters** for each of these options by using your mouse to single-click on the **Option** Name.

Action Taken on Event Match Option

By default, all newly configured Event Watcher Rules *automatically forward* **Event Matches** to the nFX Log One Server. If you want to discard an **Event Watcher Rule** and not send this information across your enterprise's network, do the following:

1. From the **Event Watcher Config** screen, in the lower right **Event Watcher Rules Options** pane, select **Action Taken On Event Match**.
   - » The **Action Taken On Event Match** pop-up displays.
2. Select either the **Forward Event To Server** or **Discard The Event** radio buttons.
3. Click **OK**.



Figure 36: Action Taken on Event Match screen

Corrective Action Selection Option

The **Corrective Action Selection** option allows you to configure nFX Log One to execute a custom script or batch file if a particular Event was *written* to a **Windows Event Log**.

Important

For your use, nFX Log One is shipped with one script file called **send_net_msg.bat**, which you can configure to send a Pop-up Message to any computer should a particular Event occur.

To apply this **Corrective Action**, you must configure **two arguments** to be passed to this script file using the **Command Line** field.

For example:

FILESERVER - "A logon failure has occurred with the Administrator account."

The computer name does not require the **** in front and the message text must be enclosed with quotation marks.

Important

You can configure nFX Log One to execute any custom script or batch file, but the file must be introduced to nFX Log One using the **Corrective Actions** option found in nFX Log One's **Setup** Utility so the script can be correctly called.

Event Acknowledgment Option

Event Rules can be configured to provide a resolution and send acknowledgement emails to **Admin** or **Help Desk** groups.

If you want nFX Log One to enable **Event Acknowledgment** for Rules:

1. From the **Event Watcher Confg** screen, in the lower right **Event Watcher Rules Options** pane, select **Event Acknowledgement**.
   - » The **Event Acknowledgement** pop-up displays.

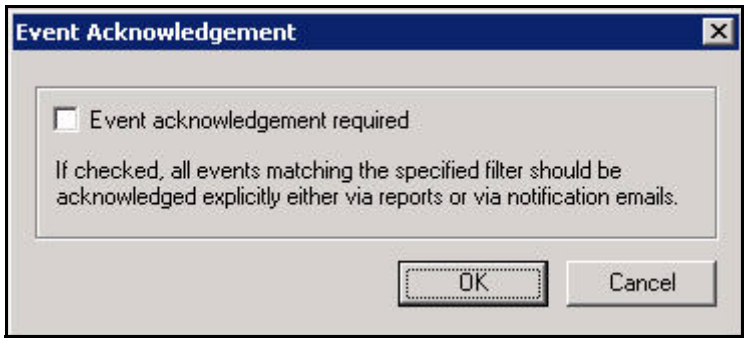


Figure 37: Event Acknowledgement pop-up

2. Click the checkbox **Event acknowledgment required**.
3. Click **OK**.

Event Routing Information Option

To choose a routing destination for alerting purposes:

1. From the **Event Watcher Config** screen, in the lower right **Event Watcher Rules Options** pane, select **Event Routing Information**.

   » The **Event Routing Information** screen displays.

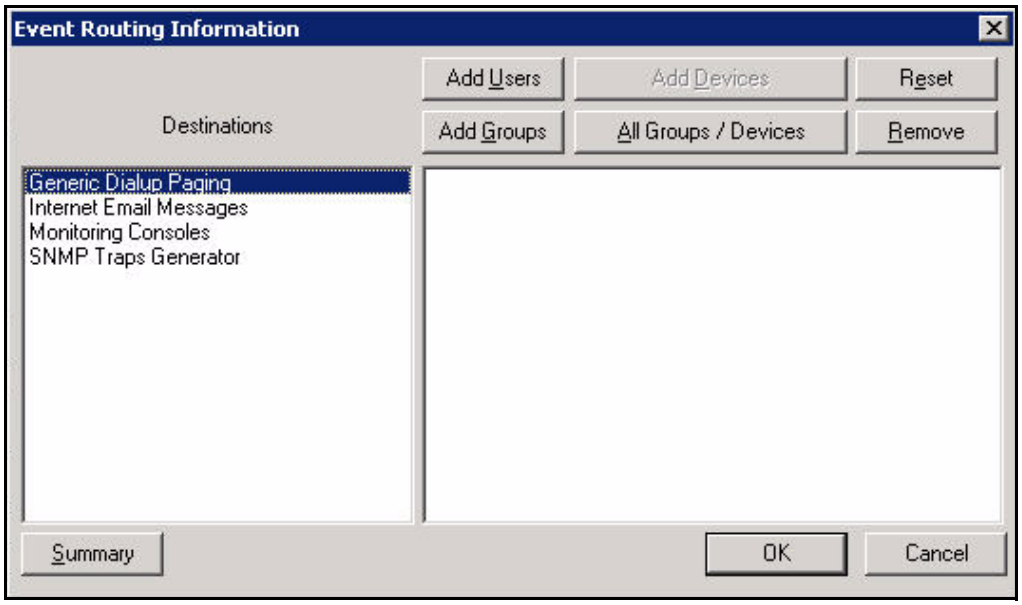


Figure 38: Event Routing Information dialog-box

2. Choices for **Destinations** are:
   - Generic Dialup Pager
   - Internet E-mail Messages
   - Monitoring Consoles
   - SNMP Traps Generator
3. Highlight the **Destination** from the **Destinations** section.
4. Select either the **Add Users** or **Add Groups** buttons to select where you would like the **Event Information** routed.
5. Select the **Users** or **Groups**.
6. Click **OK** to return to the **Event Routing Information** pop-up.
7. Click **OK** when finished.

Important

By default, The **Monitoring Consoles** destination is configured to route Event Information to **All Instances**. **All Instances** means that the **Event Information** will be sent to each User's **Console Profile**, as defined in **Setup**. In other words, nFX Log One will keep count of Events (or records) that have been viewed by each user defined in the **User Definition** section of **Setup**. This database includes the last 1,200 Events not previously viewed by each individual user. If you would like to route a particular Event to just one User's Console, select an **Individual User** rather than **All Instances**.

Important

To get a **Properties View** of the **Routing Destinations** configured for a particular Rule, click the **Summary** button located at the bottom of the **Event Routing Information** pop-up.

Warning

Be very careful when selecting the **All Groups/Devices** button as this will route the event information to all users and all devices. It is recommended that you select the Users and Devices individually until you are familiar with the routing of Event Rules.

Frequency of Notification Option

The **Frequency of Notification** option defines how often a notification should be generated. In other words, it allows you to tell nFX Log One when and how often you would like to be notified of repeated similar **Event** types.

Important

Carefully controlling notification frequency is an important part of preventing notification overload as too many notifications could easily desensitize users to the urgency of a particular problem.

1. From the **Event Watcher Confg** screen, in the lower right **Event Watcher Rules Options** pane, select **Frequency Of Notification**.
   - » The **Frequency of Notification** pop-up displays.

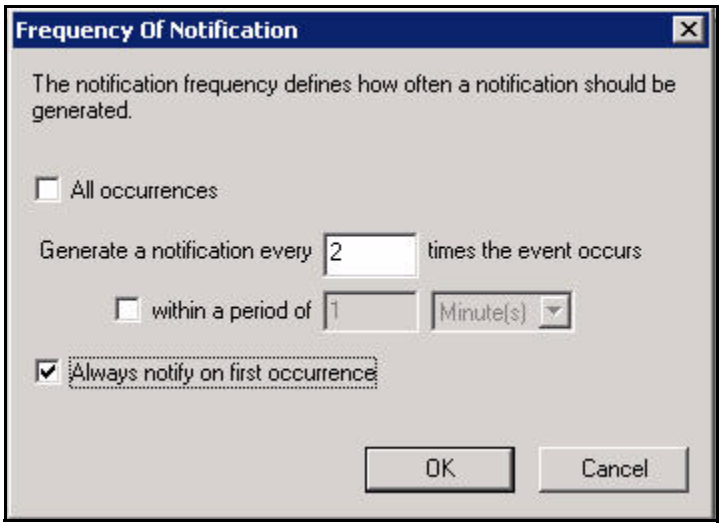


Figure 39: Frequency Of Notification pop-up

2. Here, you can perform the following functions:
   - By **selecting** the **All occurrences** checkbox, nFX Log One will route the Event **each** time the Event matches a Rule.
   - By **deselecting** the **All occurrences** checkbox, you can manage **how often** nFX Log One sends an Alert based on time and frequency.
   - In order to have nFX Log One **always notify** you the first time an Event occurs, select the **Always notify on first occurrence** checkbox.
3. When done, click **OK**.

Message Text Option

The **Message Text** option is a quick and convenient way to see the Event's **Message Text** associated with a specific Rule. The **Message Text** option can also be used to Copy and Paste information for the renaming of **Event Watcher** rules.

Notification Schedule Option

The **Notification Schedule** option allows you to determine the time of day as well as the day of the week that a specific Rule will be active. The *highlighted* hours (shown below) are the hours during which a filter is **active**. Select the **Toggle Working Hours** button to configure normal work hours and days. **Note:** By default all Rules are enabled 24/7.

1. From the **Event Watcher Confg** screen, in the lower right **Event Watcher Rules Options** pane, select **Notification Schedule**.

   » The **Notification Schedule** pop-up displays.

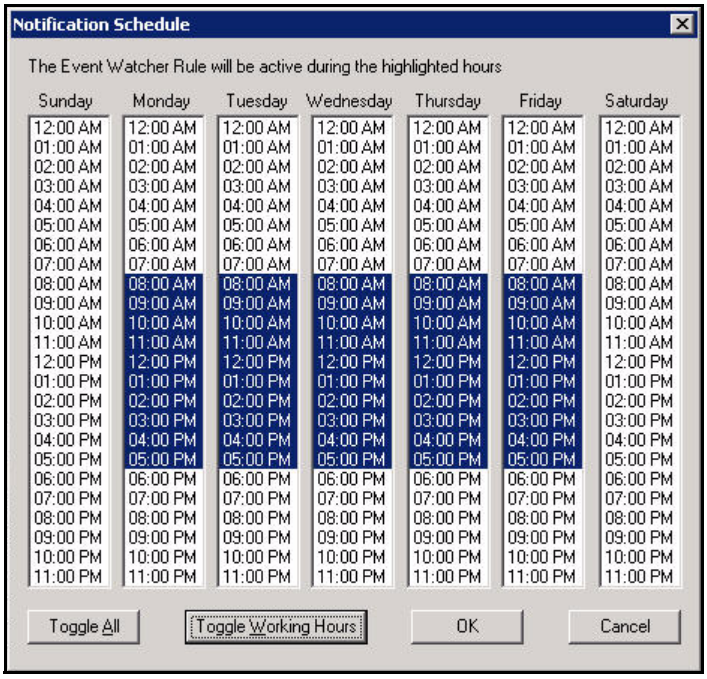


Figure 40: Notification Schedule pop-up

2. Select the **Toggle Working Hours** button to configure normal work hours and days. Or manually select hours with the mouse. **Note:** By default all Rules are enabled 24/7.
3. When done, click **OK**.

Priority of Notification Option

The **Priority of Notification** option allows you to *rank* the importance of a **Notification** based on a scale from 0 to 100, with 0 being the most important and 100 being the least important.

1. From the **Event Watcher Confg** screen, in the lower right **Event Watcher Rules Options** pane, select **Priority Of Notification**.

» The **Priority Of Notification** pop-up displays.

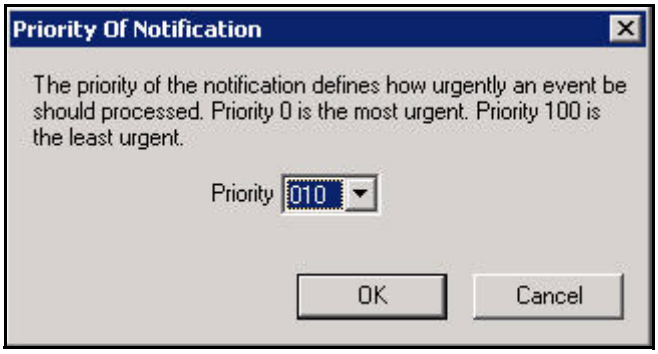


Figure 41: Priority Of Notification pop-up

2. Select the **Toggle Working Hours** button to configure normal work hours and days. Or manually select hours with the mouse. **Note:** By default all Rules are enabled 24/7.
3. When done, click **OK**.

Resolution Option

To assist users in resolving conditions, the **Resolution Text** option allows you to customize message text or instructions to the end of an **Alert**.

1. From the **Event Watcher Confg** screen, in the lower right **Event Watcher Rules Options** pane, select **Resolution**.

» The **Resolution Text** pop-up displays.

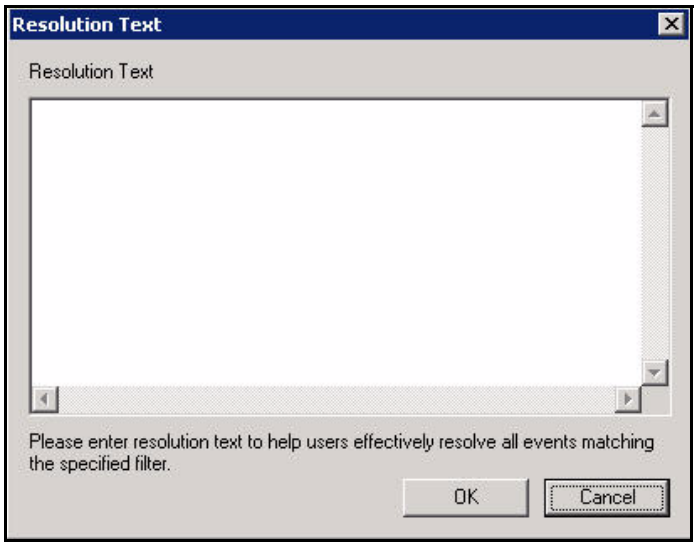


Figure 42: Resolution Text pop-up

2. Type in any desired resolution text to assist users in resolving conflicts.
3. When done, click **OK**.

Text Based Rules Option

The **Text Based Rules** option allows you to add additional criteria to the configured Rule. **Note:** Without the **Text Based Rules** option, nFX Log One only checks the **Rule Criteria Based on Header** settings to consider the rule to be a match.

By adding **Text Based Rules** or **Keywords**, nFX Log One *will not* consider the Rule to be a match unless either the Text String or all of the Keywords are *present* in the Event's Message Text.

Important

Text Based Rules can be applied to **Notification** and **Discard Rules**. Additionally, certain pre-configured Rules are *configured* with **Triggers** to help prevent your logs from filling up too quickly. Specifically, **Triggers** have been applied to logs generated from **Microsoft Security Events**, in which many identical logs are generated with only specific ID numbers being different. nFX Log One's **Trigger** functionality allows the Rules to be stored with an incremental counter instead of taking up a table entry for each individual **Event**.

1. From the **Event Watcher Confg** screen, in the lower right **Event Watcher Rules Options** pane, select **Text Based Rules**.
   - » The **Text Based Rules** pop-up displays.

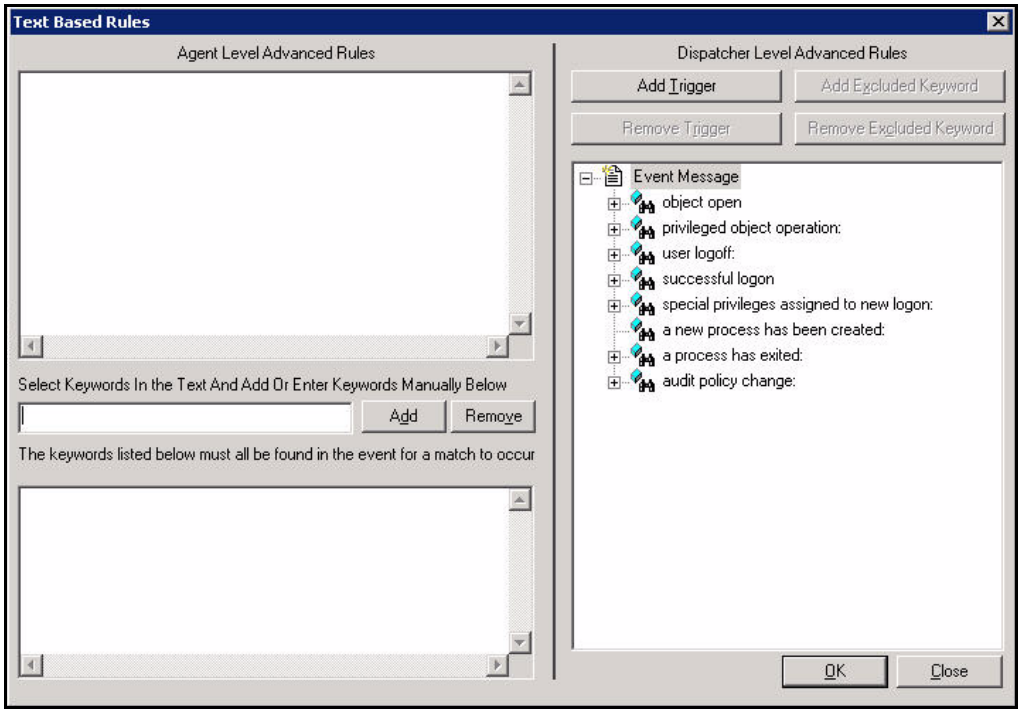


Figure 43: Text Based Rules pop-up

2. Set up **Keywords** and **Triggers** accordingly.
3. When done, click **OK**.

Creating a New Custom Event Watcher Rule

In order to create a new **Custom Event Watcher Rule** follow these steps:

1. From the **Event Watcher Confg** screen, **right-click** on any text in the **Event Watcher Rule Description** pane.
   - » A right-click menu appears.
2. From this menu, select **New Event Watcher Rule**.
   - » A new Rule Entry, titled "**<User Defined Rule>**", displays at the bottom of the list.
3. **Right-click** on the **<User Defined Rule>** and select **Move Event Watch Rule to Top**.

4. If necessary, scroll the list to the top to view the **<User Defined Rule>**.
5. Rename the rule by **right-clicking** on the rule and selecting **Rename Event Watcher Rule**.
   - » The **Rename Current Event Watcher Rule** pop-up displays.
6. Type in the name of the rules in the **Description** field.
7. Click **OK**.
8. Click the **Manual Entry** button at the bottom of the screen to configure your own custom Event Rule parameters.
9. When finished, click the **Apply** icon located on the nFX Log One toolbar to update the nFX Log One Database with the new **Rule** parameters.

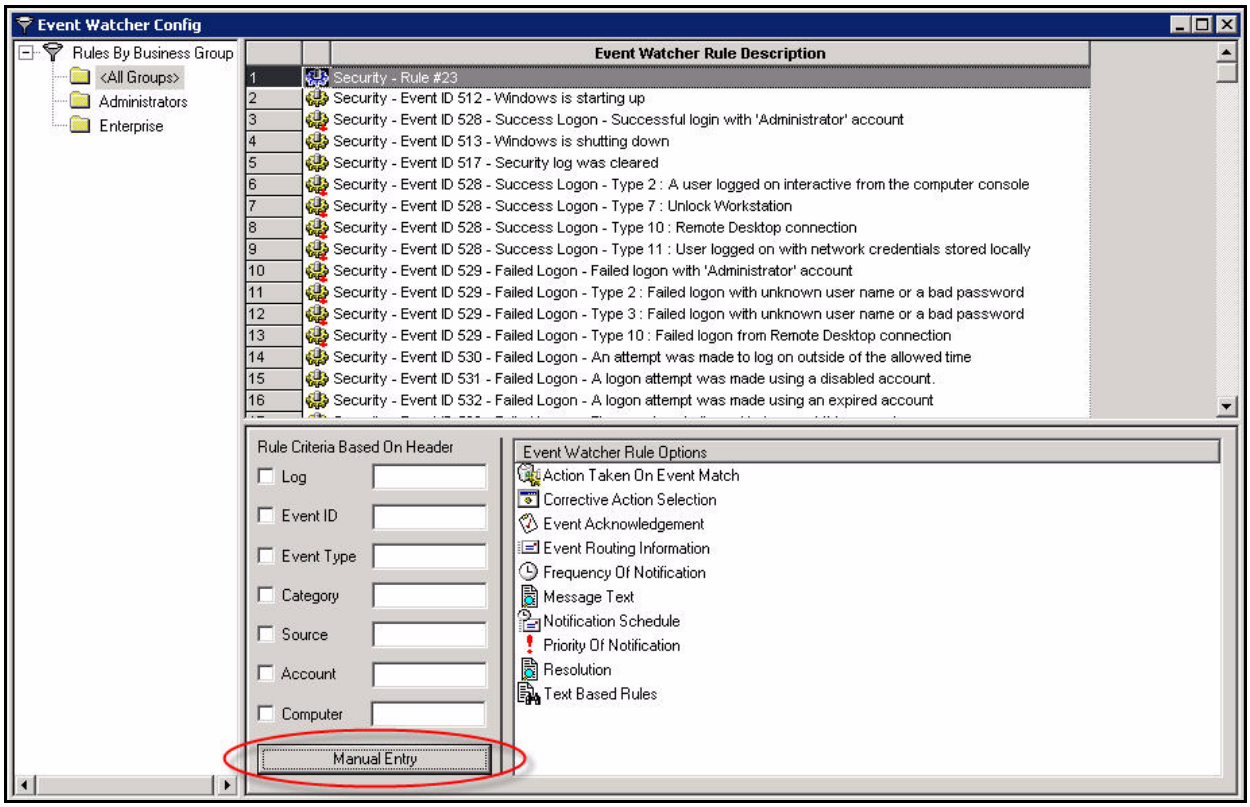


Figure 44: Event Watcher Config Manual Entry button

SysLog Watcher

The **SysLog Watcher** can be configured to receive Syslog messages from any device that can send Syslog messages such as routers, switches, firewalls, UNIX, AIX, and Linux systems.

The **SysLog Watcher** *listens* over **User Datagram Protocol** (UDP) Port 514 by default and *translates* or parses all received messages before storing to the nFX Log One database. These messages are also normalized for viewing in the Live Events viewer of the nFX Log One console. The **SysLog Watcher** can also be configured to listen on TCP port 514 if your device is setup to deliver the messages using TCP protocol.

The **Syslog Watcher** can also be configured to save all received messages in raw format to a log file for backup and archiving purposes. The default folder for the syslog raw format log file is:

`C:\Program Files\netForensics\nFX Log One\bin\Agent_Home\Repository`

If the agent is setup to manage logs (see "Log Management and Archiving" on page 36) on the Syslog receiver system, the log files will be signed, encrypted and compressed by default before archiving to the **Log Management Archive** system. There will be a folder with the device name located in the designated archive folder.

Syslog messages can also be routed at real time for alerting purposes.

Creating a SysLog Watcher Rule

1. From the nFX Log One Console menu, select ***Go > SysLog Watcher Config***.
   - » The **Syslog Watcher Config** screen displays.

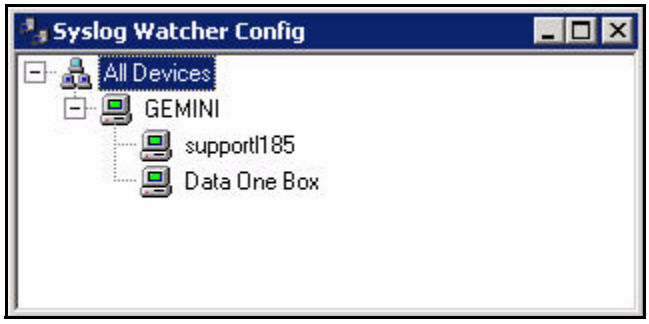


Figure 45: Syslog Watcher Config screen

2. **Right-click** on **All Devices**.
3. From the right-click menu, select **New SysLog Device**.
   - » The **Syslog Device Properties** pop-up displays.

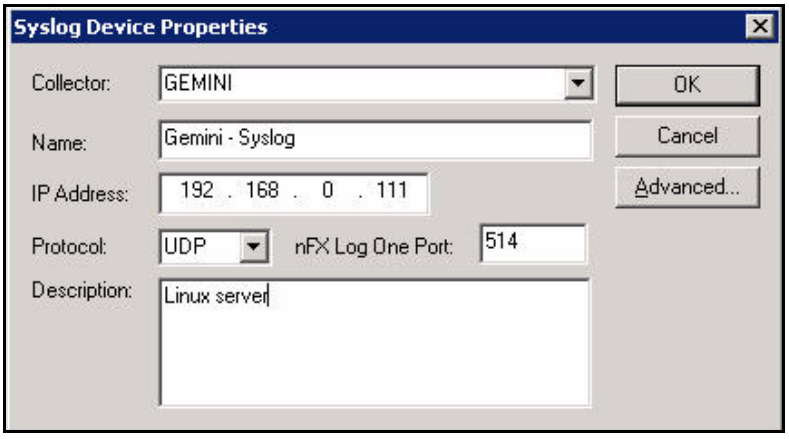


Figure 46: Syslog Device Properties pop-up

4. Enter the **Device Name** in the **Name** field.
5. Enter the Device's **IP Address** in the **IP Address** field.
6. Enter the **UDP Port Number** in the **nFX Log One Port** field.
7. Enter the Device's Description in the **Description** text box. You can also enter the function of the device in this text box.
8. Click the **Advanced** button.

» The **Advanced Properties** pop-up displays.

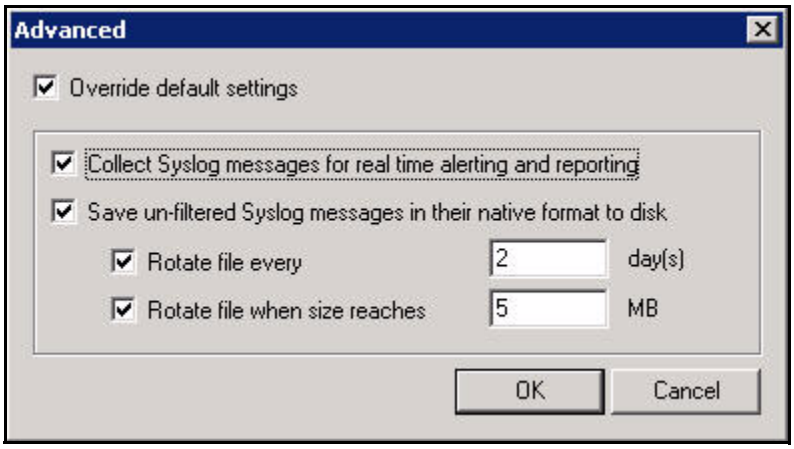


Figure 47: Advanced Properties pop-up

9. In the **Advanced Properties** pop-up check the appropriate boxes for collecting and saving the raw **Syslogs Events** to files, which can then be signed, compressed, encrypted, archived and validated at a later date using nFX Log One's Log Management features.
10. Click the **OK** button to return to the **Syslog Device Properties** pop-up.
11. Click **OK** to record the changes.

» The newly added device(s) now display in the tree under **All Devices**.

Important

On the device that you wish to monitor, you must also reconfigure the **sysconf** or **host file** with the **Name** and **IP Address** of the nFX Log One Server. For example: **New Syslog Host\\Fileserver 192.168.29.10**.

Basic Syslog Settings

Here are the basic settings required to get the *nix device (i.e., UNIX or Linux) to send syslogs messages to the nFX Log One Server. Depending on the version of *nix the locations of the files may be different.

Sample Syslog.conf

Edit /etc/syslog.conf (or where ever syslog.conf exists)

```
# Add the following lines
# Replace 10.0.0.12 with the
# IP address of nFX Log One
# Send syslogs to nFX Log One
# Note: do not use any spaces, use tabs only.

*.err           @10.0.0.12
*.crit          @10.0.0.12
auth.*          @10.0.0.12
authpriv.*      @10.0.0.12
cron.*          @10.0.0.12
```

```
#now restart syslog
/etc/init.d/syslog restart
```

***.err** = tells syslog to send **all errors** to nFX Log One
***.crit** = tells syslog to send **all criticals** to nFX Log One
auth.* = tells syslog to send **all authentications** to nFX Log One
authpriv.* = tells syslog to send **all authentications** to nFX Log One
cron.* = tells syslogs to send **all scheduled tasks** (cron) to nFX Log One

The following is information regarding Priority levels and Facilities. Priorities levels show up in the Message text of nFX Log One Syslog Watcher Events.

Priority: debug
Priority: info
Priority: notice
Priority: warn
Priority: err
Priority: crit
Priority: emerg

Unix/Linux Facility levels are listed below

Facility: auth
Facility: authpriv
Facility: cron
Facility: daemon
Facility: ftp
Facility: kern
Facility: lpr
Facility: mail
Facility: user
Facility: uucp
Facility: level0

Facilities and Windows equivalents

Facility: auth = AUTHENTICATION
Facility: authpriv = AUTHENTICATION
Facility: cron = Job/Task Scheduler

Facility: daemon = SERVICE
Facility: ftp = FTP
Facility: kern = KERNEL / OS
Facility: lpr = PRINTER QUEUE
Facility: mail = EMAIL

Performance Watcher

This section reviews the configuration of the **nFX Log One Performance Watcher** and describes how performance information can be viewed in real-time.

Performance Watcher items are organized as follows:

- What is the **Performance Watcher**?
- Configuring **Performance Watcher Alerts**
- Creating an **Application Template**
- Defining the **Performance Threshold**
- Applying **Performance Templates** to Systems
- Importing and Exporting **Performance Watcher Templates**
- Using the **Live Performance Watcher**

nFX Log One Performance Watcher

Performance Watcher allows nFX Log One to alert the user when a **Windows NT/2000/2003/XP** performance counter breaches a user-defined threshold. Performance counter monitoring is performed at the **nFX Log One Agent** level so monitoring overhead is minimal.

In the event of a breach, a user-defined **Event** is generated in the **Windows Event Log**. Using the existing routing capabilities of nFX Log One the Event can be routed via e-mail, pager, etc.

Important



To monitor disk related performance counters, you must first activate the counters in **Windows**. To do this, go to a command prompt and enter **diskperf -Y**.

Configuring Performance Watcher Alerts

Performance Watcher monitors Windows and application performance counters and alerts you if these counters exceed a user-defined threshold. These counters (alone) provide you with an indication of the performance of many of the aspects of computer management. nFX Log One adds value, however, by adding the ability to alert you to critical events occurring on you organization's network.

Important



nFX Log One manages the performance monitoring by grouping performance counters into a template and applying user-defined thresholds to these counters. These templates can then be applied to individual machines or groups of machines.

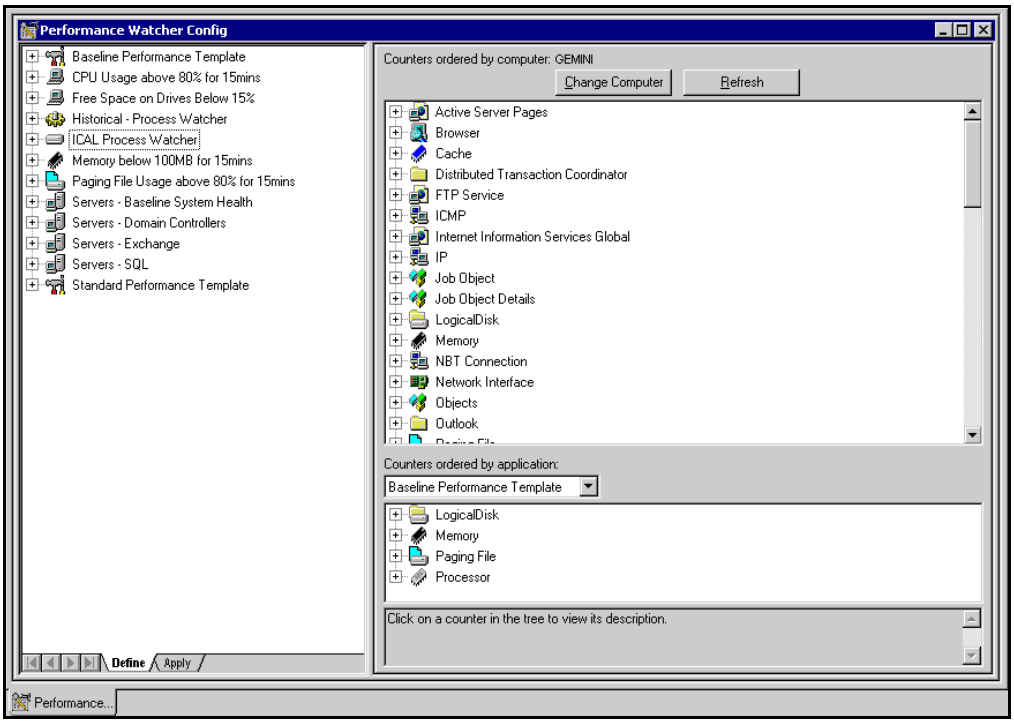


Figure 48: Performance Watcher Config screen

To Configure a Performance Watcher Template

To create a template, follow the steps below:

1. Select ***Go > Performance Watcher Config*** from the nFX Log One main toolbar.
   - » The **Performance Watcher Config** screen displays.
2. To rename the template, **right-click** anywhere in the left pane of the screen and select **New Template**.

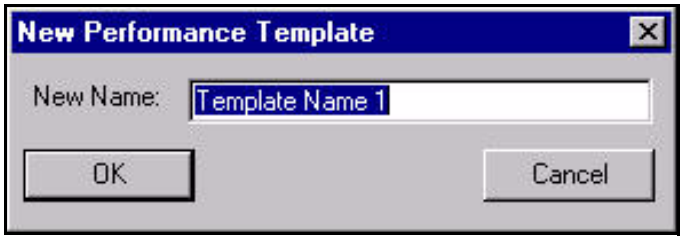


Figure 49: New Performance Template dialogue

3. Enter the name of the Template in the **New Name** field.
4. Click the **OK** button.

To Configure the Server Update Frequency

The **Server Update Frequency** must be configured for any **Template** that can be enabled in the **Collection** tab. The **Server Update Frequency** is the rate which the Agent machine or machines push the historical data that is being sampled over to the **nFX Log One Server**.

To configure the **Server Update Frequency**, follow these steps:

1. From the **Performance Watcher Config** screen:

a. **Right-click** on the **Template Name** and select **Properties**.

b. **Double-click** on the **Template Name**.

» The **Template Data Collection Settings** dialogue box displays.

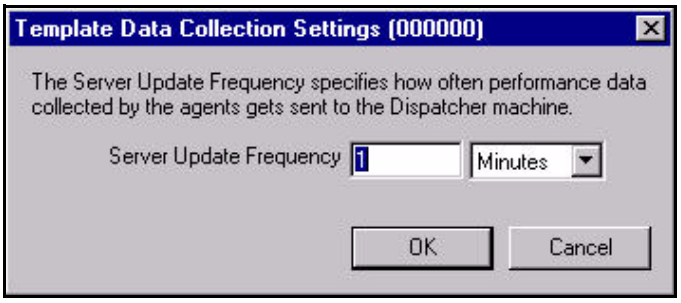


Figure 50: Template Data Collection settings dialogue

2. Set the **Server Update Frequency** to the desired rate.

3. Click the **OK** button.

Creating an Application Template

If you are running specific applications that load their own performance counters, then you can use **Application Templates** to create a specific template with those counters. If you do not have the specific application installed on the machine in which you are configuring the **Templates**, those counters will not be displayed. With this option, you can create an **Application Template** and apply it to all of the machines that are running that particular application. This is particularly helpful for users of applications such as, **MS Exchange**, **MS SQL Server**, **MS SMS**, etc. This can also be used for any in-house application that generates its own performance counters.

To Create a New Application Template

Follow the steps below to create a new **Application Template**:

1. First, create a new **Template** and rename the **Template**. It is recommended that you rename the **Template** to recognize it as an **Application Template**.

2. Locate the new **Template** in the **Template** list and **right-click** it.

3. Select **Is an Application Template** from the right-click menu.

» The **Template** displays in the **Counters Ordered by Application** box. When you add in counters as described in the **Configuring Performance Watcher Alerts** section, you should see that the counters have been added in both screens.

Defining the Performance Threshold

Defining a **Performance Counter Threshold** allows you to be alerted through nFX Log One if a user-defined threshold is breached for a specific time period. This forces nFX Log One to generate an **Event** in the **Windows Event Log** that is forwarded to the nFX Log One Console and other routes that have been defined, such as pager, e-mail, etc.

Once you have created a **Performance Template**, click on the **Template** name in the list to expand the **Template** and view the counters you have chosen to comprise your **Template**. Double-click the counter name itself to launch the interface allowing you to define its threshold.

Important

The **Counter Properties** window is divided into two tabs: **Collection** and **Alert** Configuration.

Collection

The **Collection** tab on the **Counter Properties** screen allows historical performance data to be efficiently collected from any system with an **nFX Log One Agent** installed. The collection frequency, time of day, performance counters, and frequency that the **Agents** forward data to the **nFX Log One Server** are user-definable. The nFX Log One Server stores this data for creation of historical **Performance Reports**.

1. Right-click on the template and select **Properties**.
2. Select the **Collection** tab.
3. Click the **Enable Data Collection** checkbox to activate the **Counters Properties** dialog.

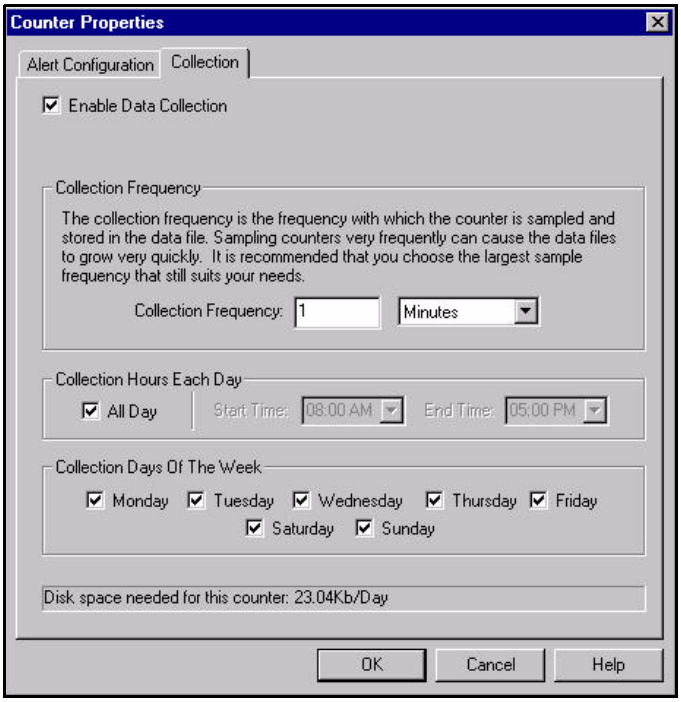


Figure 51: Counter Properties: Collection tab

1. In the **Collection Hours Each Day** box, select the time duration that you would like the selected **Performance Counter** to be sampled. If you select the **All Day** option, the selected performance counter is sampled 24 hours a day. If you select the **Start Time** and **End Time** options, the **Performance Counter** selected is only sampled during the set time duration.
2. In the **Collection Days of the Week** box check the days of the week that you would like the **Performance Counters** to be sampled.

Important

The amount of disk space required for each **Performance Counter** is estimated and displayed at the bottom of the **Collection** tab. If any of the above options are changed, then this estimate will also change dynamically.

Alert Configuration

The **Alert Configuration** tab on the **Counter Properties** screen enables you to determine the threshold for the counter. When this threshold is exceeded, nFX Log One writes an **Event** in the **Windows Event Log** that is forwarded to the **nFX Log One Console**.

Use the drop-down menus on the **Counter Properties** screen to select the appropriate parameter for the counter you are configuring.

For example:
If you are configuring a **Performance Counter** that is measuring a percentage, simply enter the number corresponding to the percentage that you would like.
If you are configuring a Performance Counter that is measuring seconds, bytes, etc, simply enter the value that you would like.

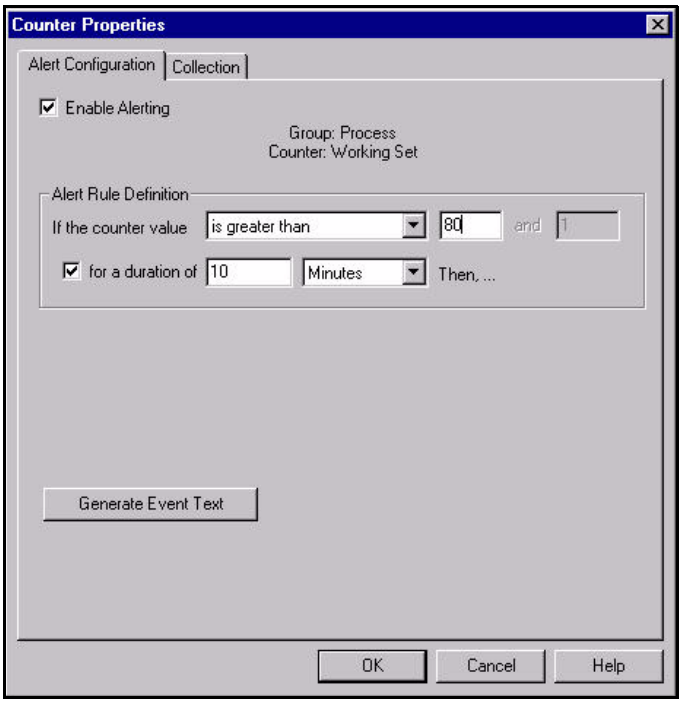


Figure 52: Counter Properties: Alert Configuration tab

Use the **Generate Event Text** button to specify what text you would like generated within the Event created when the threshold is exceeded, and when the counter has returned to normal operating range.

To Configure Default Performance Counter Properties

Creating **Default Performance Counter Properties** allows you to configure default properties to be applied to new **Performance Templates**. This greatly reduces the amount of time needed to configure multiple **Performance Counters** with the same properties. The new default properties will only be applied to new **Performance Templates**. Any previously configured templates will NOT be affected.

This option applies the preferences on a per user basis. Therefore, all users may not have exactly the same **Performance** properties configured. To configure, follow these steps:

1. From the nFX Log One toolbar, select ***View > Preferences***.
2. Click on the **Performance** tab.
3. Click the **Properties** button.
   - » The **Counter Properties** screen displays.

4. Configure the **Alert Configuration** and **Collection** tab with the properties that you would like to apply to **all** of the **Performance Counters** in the future.
5. When finished, click **OK**.

Applying Performance Templates to Systems

Once you have created **Performance Templates** and defined the thresholds of the counters comprising the templates, you are ready to apply the templates to your monitored systems or groups.

1. From the **Performance Watcher Configuration** screen, select the **Apply** tab at the bottom of the window.
2. **Drag and drop** the Computer or Group Name onto the Template that you would like to apply.
3. Click the **Apply** icon on the nFX Log One toolbar to save your changes to the nFX Log One database and activate the **Performance Watcher**.

If the **Performance Counter** being added has multiple instances, the **Instance Chooser** box will appear. Select the instances that you would like to monitor by clicking on the corresponding check box. If you would like to select all, then click **Check All**.

Using the Live Performance Watcher

Once you have added **Counters** to a **Performance Template**, you can then view those counters in the **Live Performance Watcher** by following these steps:

1. From the nFX Log One toolbar, select click the **Go > Live Performance Watcher**.

Important

You do not need to have the **Live Performance Watcher** up in order for your **Performance Watcher thresholds** to be monitored. Once the templates have been pushed out, nFX Log One works as a service in the background; it immediately monitors configured counters, and will generate Events if your thresholds are exceeded.

Important

As the **Live Performance Watcher** launches for the first time, you will be prompted to define the counters you wish to view.

Follow the steps below to add a counter to the current **Template** view:

1. **Right-click** in the **Viewing** Area and select **Add Counter**.
2. You will need to select the **Template** to view the counters on that system. nFX Log One will adjust the rest of the fields to match the Template you have selected. If you would like to view all of the Templates according to computer or business group, then select the corresponding option.

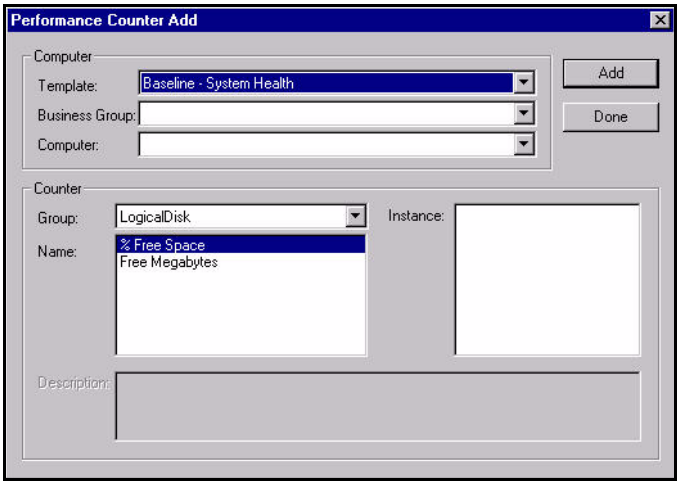


Figure 53: Performance Counter Add screen

3. In the **Counter** section, select the **Group** option if you have added more then one type of group to the **Template**.
4. In the **Counter Name** field, select the counter you want to add.
5. In the **Instance** box, if applicable depending on the counter selected, highlight an **Instance**.
6. Click the **Add** button to add the selected counter to the **Performance Monitor Viewer**.
7. Continue with this process until you have selected the desired amount of counters.
8. When complete, click **Done**.

To Edit the Properties of the Live Graph

To edit the properties of the Graph:

1. **Right-click** on the Graph.
2. Select **Properties**.
   - » The **Chart Properties** screen displays.

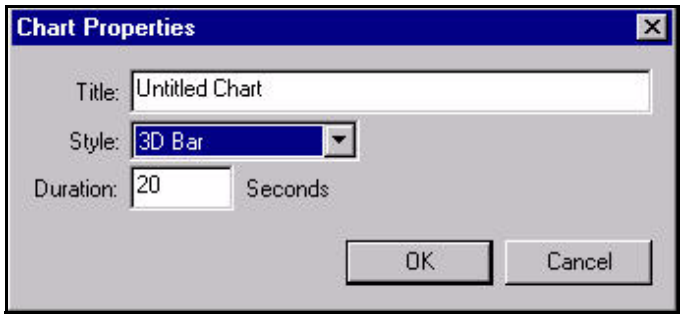


Figure 54: Chart Properties dialogue

3. Select the type or Style of **Graph** you would like to view and the amount of seconds you would like to see appear in the graph (minimum five seconds/maximum 600 seconds).

4. Click **OK**.

Important 

Depending on the type of graph selected, the amount of **Live Views** open at once, and the **Chart Duration** configured, your CPU will be affected.

Important 

It is also recommended that if you have selected a **3D** or **Area** type chart that the **Chart Duration** time not be too excessive as this will affect the visual representation of the data.

To Delete a Counter from the Graph

1. **Right-click** on the Graph.
2. Select **Remove Counter**.
3. Select the **Counter** you would like to remove.
4. Click the **Remove** button.

To Save a Live Graph

1. **Right-click** on the Graph
2. Select **Save As**.
   - » The **Save As** dialog box displays.
3. Name the Chart or accept the default.
4. Click **Save**.

To Open a Saved Performance Chart

1. **Right-click** on a Graph.
2. Click **Open**.
3. Select the File that you want to open.
4. Click the **Open** button.

To Change Performance Report Time Period

1. **Right-click** on the graph.
2. Select **Change Time Period**.
3. Enter the **New Time Period** that you would like to view.

Text File Watcher

This section introduces you to the setup and configuration of nFX Log One's **Text File Watcher**. Here you will learn:

- How to create a new text **File Watcher Rule**
- How to import and export **Text File Watcher templates**

Text File Watcher is a powerful tool that allows you to convert any text file entries into a Windows NT/2000/2003/XP event for easier monitoring. Most **Applications** generate logs for their own activity; however, these logs cannot be viewed outside of the specific Application. This can limit the usefulness of the Application Log because System Administrators cannot actively view the logs in real time or remotely from another computer.

With nFX Log One's **Text File Watcher**, you are able to generate **Windows Events** *based* on the text written to an **Application Log** or **Text File** and then utilize nFX Log One's routing to be alerted via pager, e-mail, SMTP Trap, etc. nFX Log One's **Text File Watcher** also allows you to *execute* a **Corrective Action**.

You can create individual **Text File Watcher Rules**, or create or import a **Template** which can than be applied to one or more files with the same text format.

Important

An **nFX Log One Agent** must be deployed to the system where the Text or Log File resides. The Text File Watcher can monitor multiple files under one folder using a wildcard.

Creating a Text File Watcher Rule

To configure a **Text File Watcher Rule**, you must first create a **Template** which can be applied to one or more files with the same text format.

1. From the **nFX Log One Console**, select ***Go > Text File Watcher Config*** from the menu.
   - » The **Text File Watcher Config** screen displays.

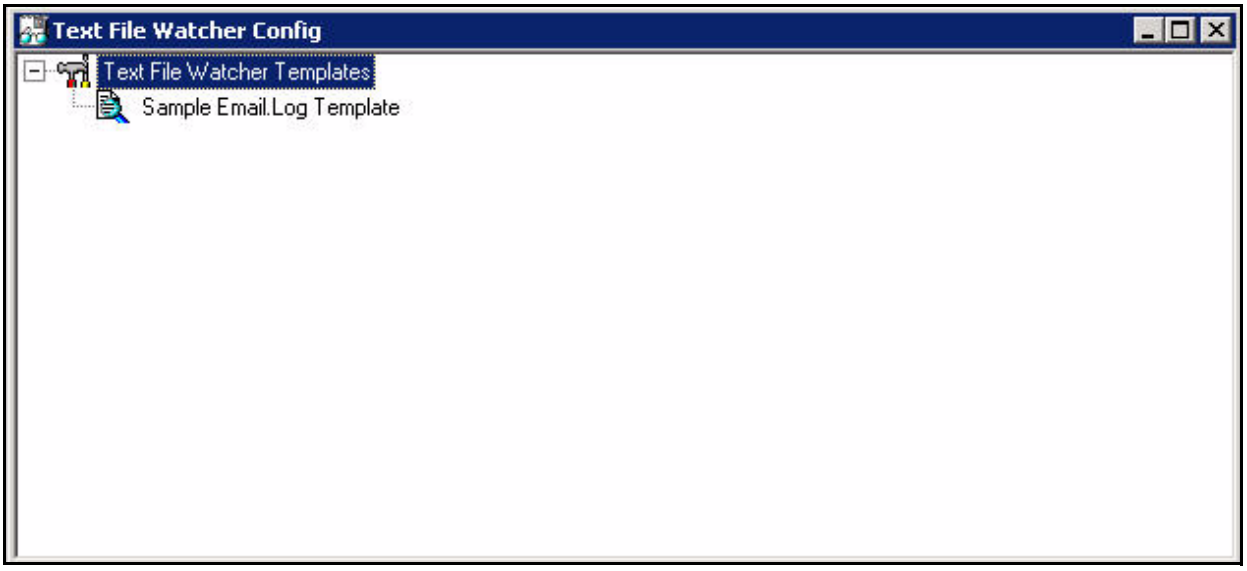


Figure 55: Text File Watcher Config. Screen

2. **Right-click** in the **Text File Watcher screen** and select **New Template**.

» The **Template File Selection** pop-up displays.

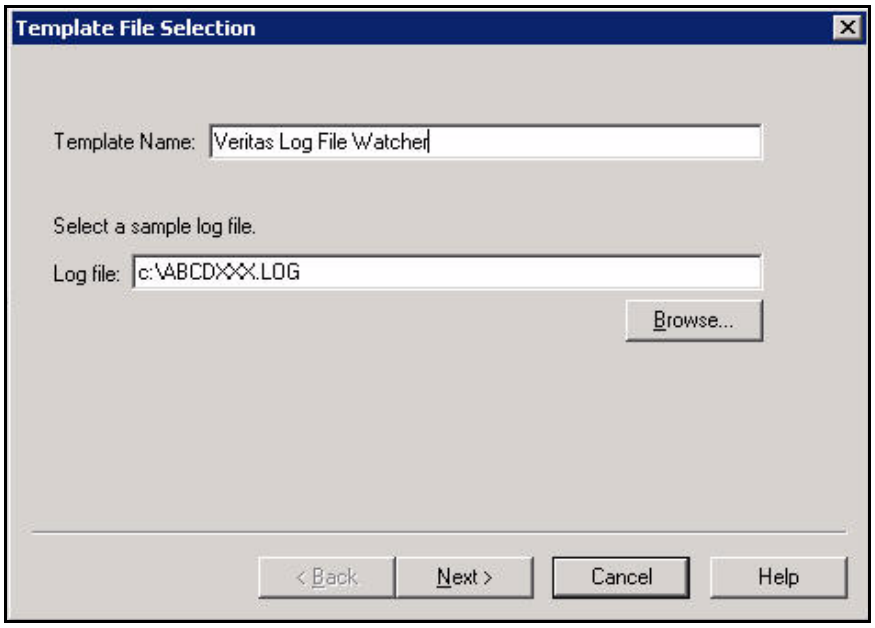


Figure 56: Template File Selection pop-up

3. Enter the name of the template in the **Template Name** field.
4. Click the **Browse** button to browse to a sample log file to use for setting up your **Text File Watcher Rule**.
5. Select the log file that you want to use.
6. Click **Open**.
7. Click the **Next** button.

» The **Log File Format** pop-up displays.

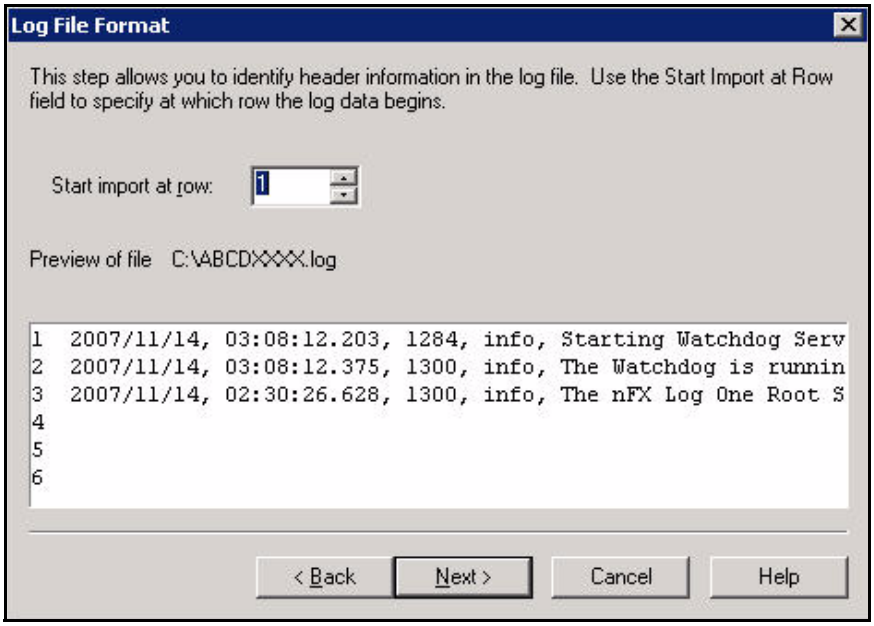


Figure 57: Log File Format pop-up

» You can now identify the Header information in the log file.

8. Click the **Start import at row** field arrow up or down to select which row within the log file you want the monitoring to begin.
9. Select the **Row**.

Important

The sample log file cannot contain more then 256 characters per line in the sample viewing area. You can manually delete characters in the sample log to allow nFX Log One to store the template into the database. Once the template is configured and saved, the actual production log file may contain lines of text with over 256 characters. Example: *.xml files.

10. Click the **Next** button.

» The **Log Files Delimiters** pop-up displays.

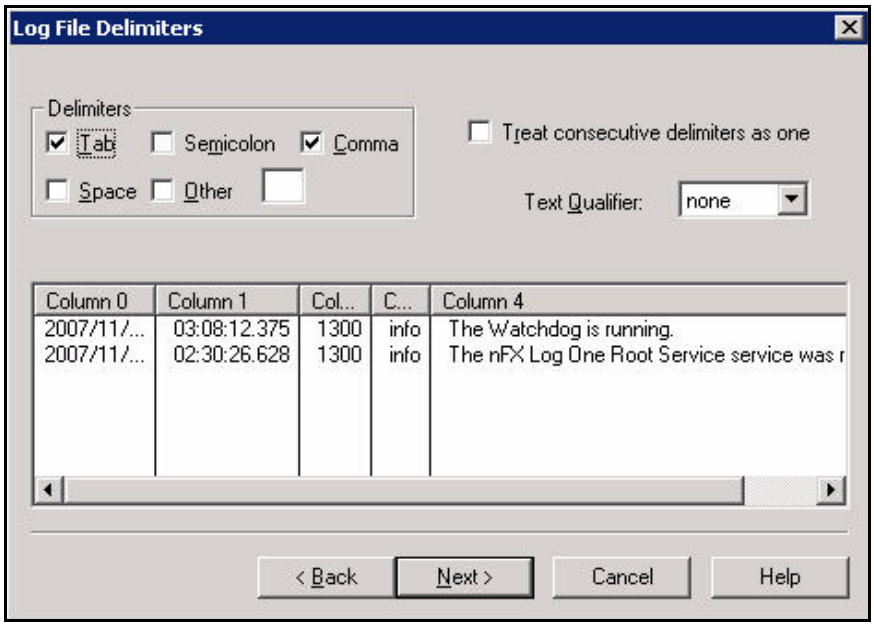


Figure 58: Log File Delimiters pop-up

11. Select which **File Delimiters** your log file uses in the **Delimiters** section of the **Log Files Delimiters** pop-up. **Note:** It is often recommended that you **DO NOT** use delimiters.
12. You can also select the **Treat Consecutive Delimiters As One** checkbox if the text file utilizes multiple delimiters in a row.
13. Select the type of **Text Qualifier** used in the file from the **Text Qualifier** drop-down arrow.
14. Click the **Next** button.

Important

The file may contain text strings that contain the delimiter. In that case, nFX Log One will ignore the delimiter.

» The **Columns Names** pop-up displays.

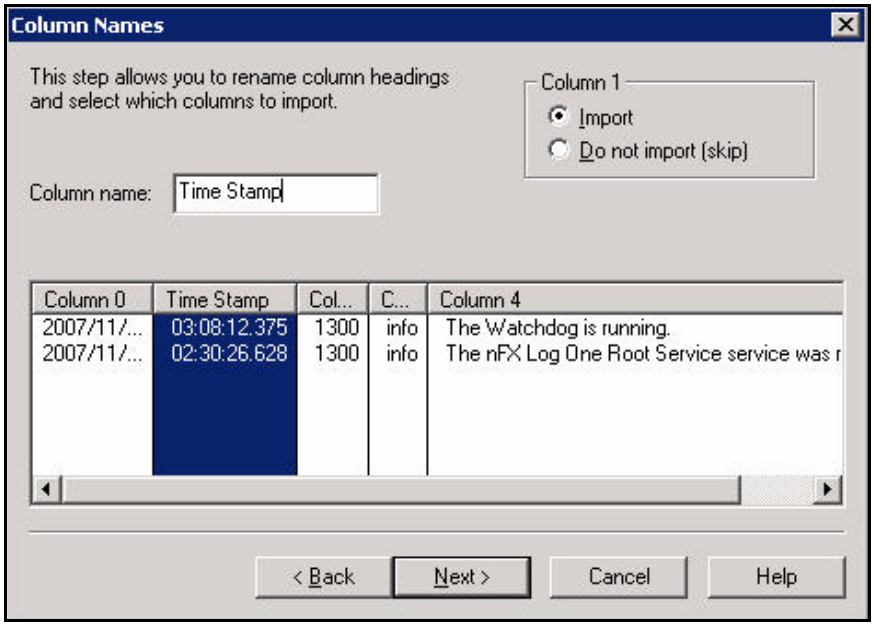


Figure 59: Column Names pop-up

15. Select the **Column** that you would like to rename from the Column Name field.
16. Rename the column in the **Column Name** text field.
17. In the **Column X** section of the **Column Names** pop-up, either select the **Import** radio button to import the selected column or select the **Do Not Import(skip)** radio button to skip this step.
18. Click the **Next** button.

» The **Event Generation Rules** pop-up displays.

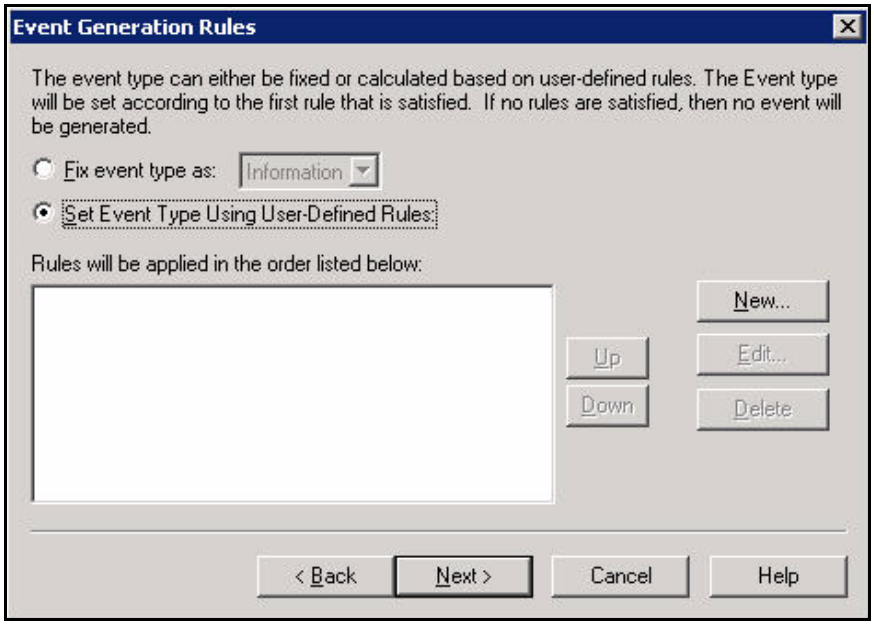


Figure 60: Event Generation Rules pop-up

19. Select the **Fix Event Type** radio button to fix a specified type of event every time a full record is written into a log file or select the **Set Event Type Using User-Defined Rules** radio button to generate an event based on the information in the log file.

    If you selected the **Set Event Type Using User-Defined Rules** radio button, you must now add the rules you would like to apply.

    a. Click the **New** button.

    » The **Event Rules** pop-up displays.

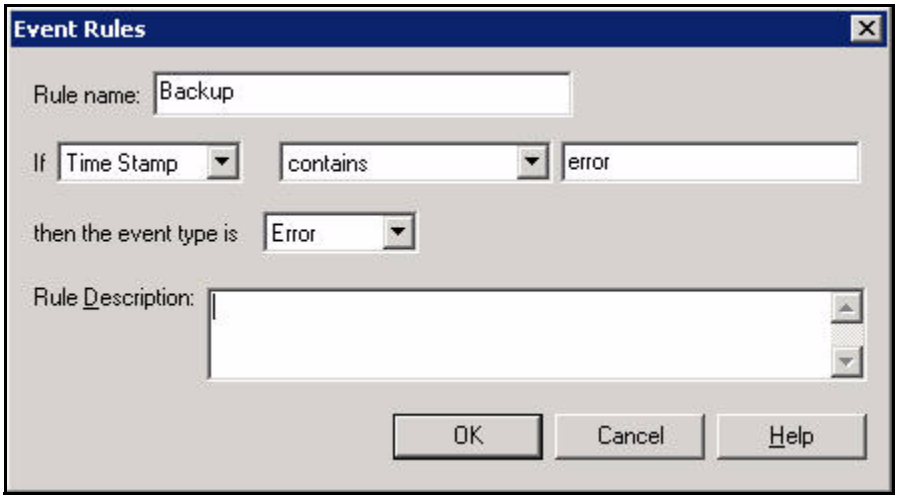


Figure 61: Event Rules pop-up

    b. Enter the new **Rule Name** in the **Rule Name** field.

    c. From the **If** pull-down menu, select the **Column Name** that you want to apply your new Rule to. Select **column 0** if no delimiters were selected.

    d. In the next field, use the pull-down arrow to select the option from the displayed list that applies to the option that you chose in the **If** field.

    e. Select the type of event you would like nFX Log One to generate when the Rule is triggered your options are: **Information**, **Warning** or **Error**.

    f. Enter **Notes pertaining to your new rule** in the **Rule Description**.

    g. Click the **OK** button.

    » The **Event Generation Rules** pop-up is visible and the new rule now appears in the rule list.

20. On the **Event Generation Rules** pop-up, click the **Next** button.

» The **Select Event Description** pop-up displays.

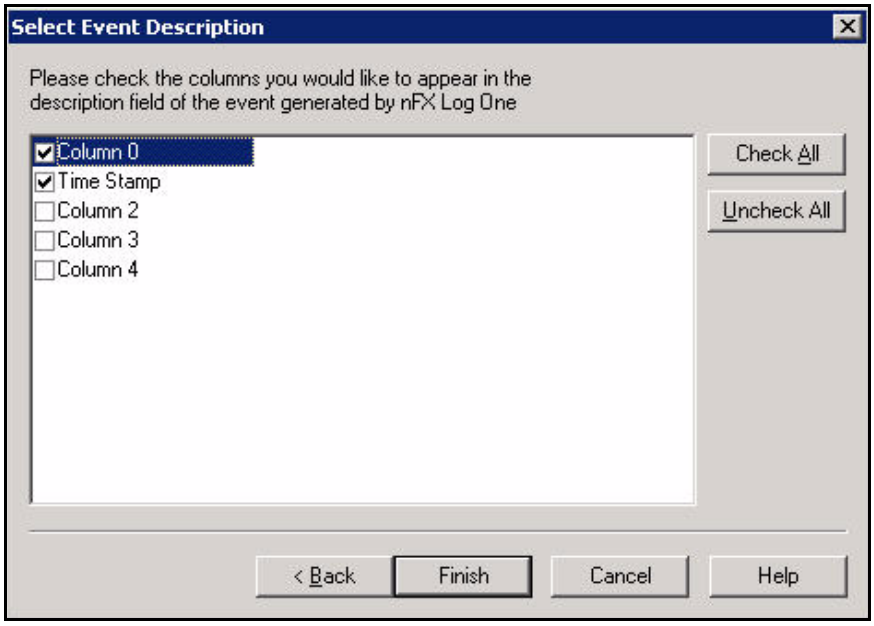


Figure 62: Select Event Description pop-up

» Here you have two choices: You can either select the checkbox next to the name of the Columns that you would like to appear in the Description field of the nFX Log One Event, or you can click the **Check All** button to select all of the Columns.

21. Click the desired checkboxes or the **Check All** button.

22. Click the **Finish** button.

» The **Text File Watcher Config** screen displays displaying the new Text File Watcher Rule.

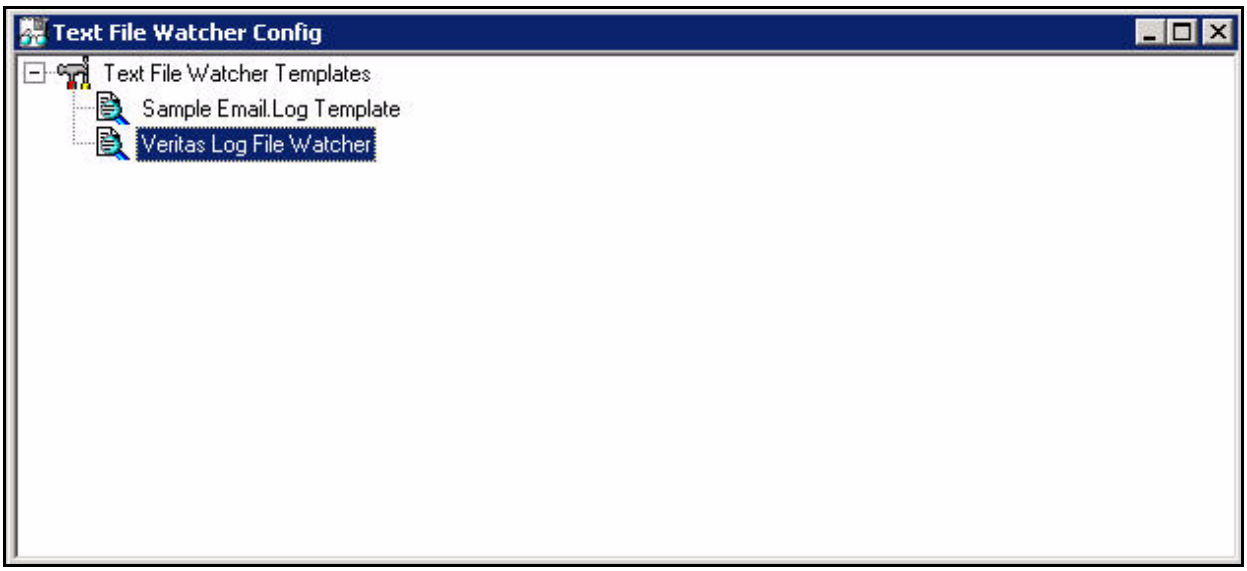


Figure 63: Text File Watcher Config screen

Now that you have created a Text File Watcher Template, you must decide which computers and files to monitor.

1. From the **Text File Watcher Config** screen, **right-click** on the new **Template** and select **New Text File Watcher**.
   - » The **Select a Computer and Files to Monitor** dialog box displays.

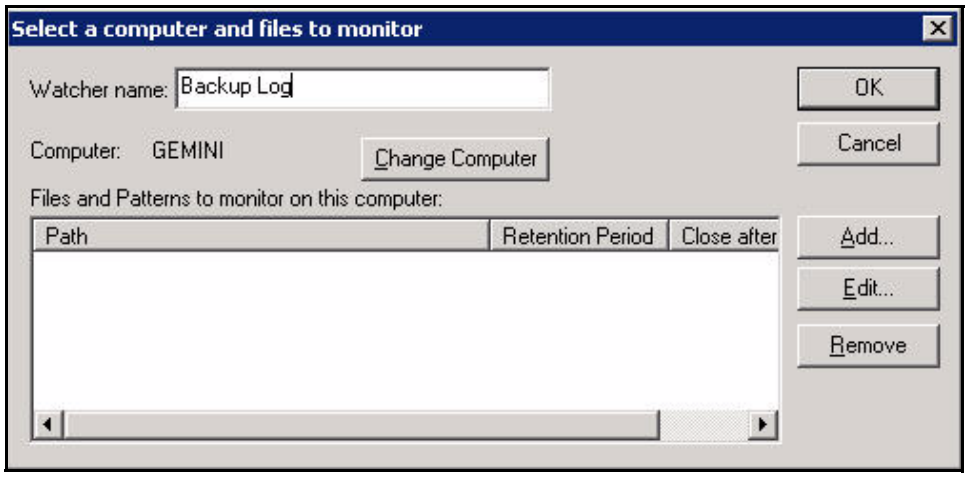


Figure 64: Select a computer and files to monitor pop-up

2. Enter the **Template Name** that you would like to use in the **Watcher Name** field.
3. Click the **Change Computer** button to select the nFX Log One Agent machine where the file the file to be monitored resides. Click **OK**.
4. Click the **Add** button to add the folder path of the file to be monitored on the selected agent machine. This is the local path as the agent would see the file. You can utilize the **'*'** wildcard as listed below to indicate to the agent that multiple files need to be monitored in this folder location.

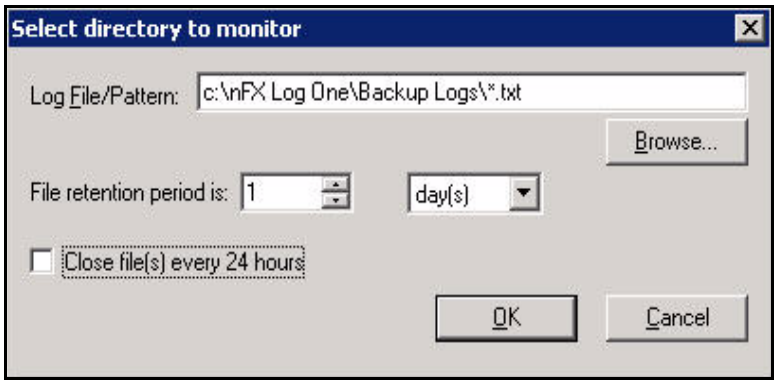


Figure 65: Select Directory to Monitor pop-up

   a. The **Close file(s) every 24 hours** check box is optional.

Important

The file retention period selection is optional and for efficiency purposes only. It is recommended to use this option if the file is rarely written to or if the file name changes daily.

   b. Click the **OK** button when you are finished with the **Select directory to monitor** pop-up.
5. Click **OK** when finished configuring the **Text File Watcher**.

6. Click the **Apply** button or ***File > Save*** to apply the **Text File Watcher** to the agent machine.

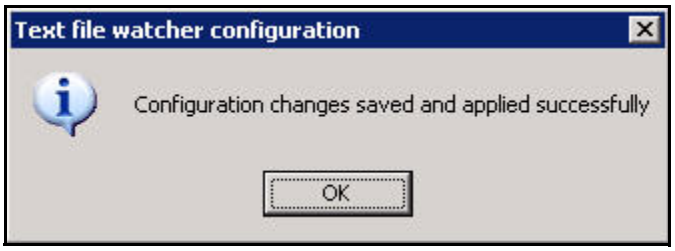


Figure 66: Text File Watcher Configuration confirmation pop-up

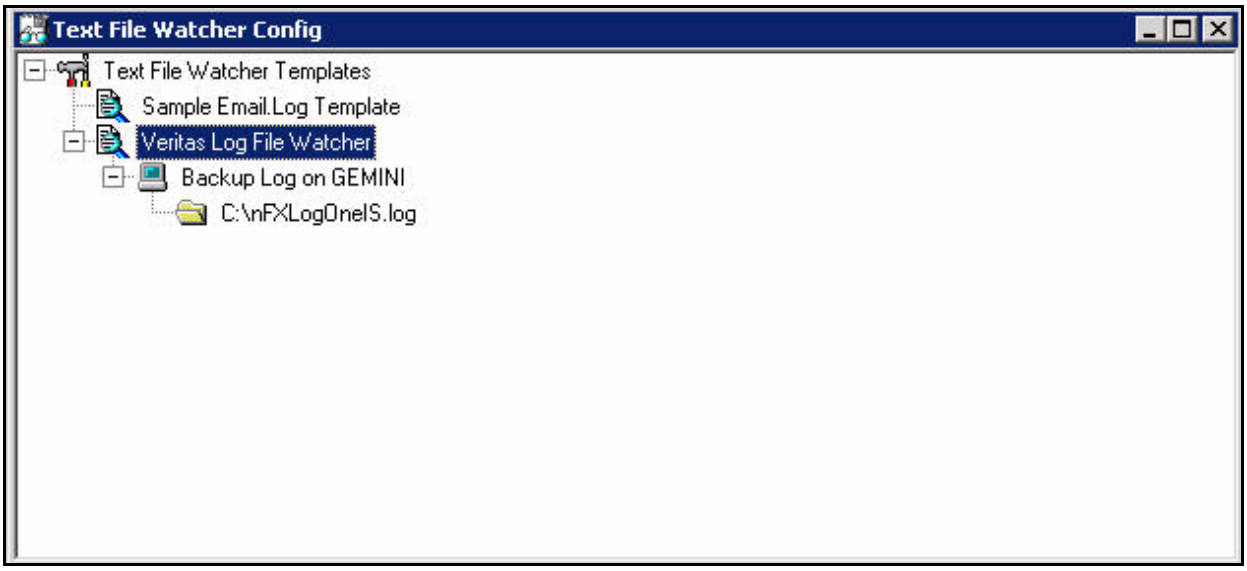


Figure 67: Updated Text File Watcher Config screen

Saving and Importing a Text File Watcher Template

The following section will instruct you on how to **import** and **export** custom **Text File Watcher templates**.

1. From the **Text File Watcher Config** screen of the **nFX Log One Console**, select ***File > Export*** and browse to your nFX Log One Files backup folder location.

   You can also select ***File > Import*** to bring your templates into the **Text File Watcher Config** screen.

2. When the file is selected, click **Save**.

nFX Log One System Management Tools

This section provides detailed information regarding the suite of management tools provided with nFX Log One. They are:

- System Management Tool Overview
- Snooze Tool
- Reboot Tool
- Run Tool
- Scheduler
- Service Control Manager
- Alert Maintenance Tool
- Database Configuration Tool
- Database Quota Management Tool
- Backup and Restore Tool

System Management Tool Overview

nFX Log One offers a complete suite of management tools that work in conjunction with basic nFX Log One functionality to ease the tasks of system and network maintenance. These tools are summarized below, and described in detail throughout this section.

- **Snooze Tool** - Allows nFX Log One to disable user-defined levels of monitoring, alerting, and corrective actions during a certain period of time so that, for example, system maintenance can be performed without erroneous alerting.
- **Reboot Tool** - Automates the rebooting of systems, and allows you to set a reboot schedule for a computer or group of computers.
- **Run Tool** - Automates the running of executables on a computer or group of computers, and allows you to set a schedule to run the executable on a regular basis.
- **Scheduler** - Provides easy access to all scheduled snoozes, reboots, run tasks, and reports.
- **Service Manager** - Allows you to control any remote or local service on any system where an nFX Log One Agent resides.
- **Alert Maintenance Tool** - Allows you to stop pending alerts from being delivered to their intended recipient. This tool is extremely useful for controlling erroneous alerting backlogged by nFX Log One on a per user basis.
- **Database Configuration Tool** - Allows you to change the database nFX Log One uses to store all historical data and configuration information.
- **Database Quota Management Tool** - Allows you to define how long data is stored on your hard drive.
- **Backup and Restore Options** -These options allow you to backup all of the nFX Log One configuration files in the nFX Log One directory. This configuration can then be restored to the same system or any other system that may have had its configuration deleted.

Snooze Tool

The **Snooze Tool** allows nFX Log One to *disable* corrective actions, scheduled reboots, alerts, and service restarts during a certain period of time. Scheduled or unscheduled maintenance can be performed on the system(s) during this time period of snoozing, without the hassle of erroneous alerting. During the snooze period, nFX Log One also generates a live view of the current and past snoozed systems in your

environment. This includes the time of day that the snooze started and ended, the duration, the user initiating the snooze, the user un-snoozing the system(s), and the reason and remarks for the snooze period. This information can then be printed to include in quarterly/yearly down time reports.

The **nFX Log One Server** maintains the timers to un-snooze and manages the updates of those timers. However, the nFX Log One Agents actually implement the snoozing.

Important

The snooze configuration files and others are located in the **\nFX Log One\bin\Eds_home\configDB** directory. The **Snooze.cfg** file is where the configuration of the **Snooze Tool** is held and the **SnoozeTimersState.dat** file is the file that contains the time left on the snooze timers. This information is important in case of an nFX Log One Server crash or shutdown, so that the snoozed machines can be un-snoozed at the scheduled times. This file is updated on a regular basis of every 10 minutes, or whenever the configuration of snooze is changed.

Configuring a Snooze

1. From the nFX Log One Console menu, select ***Tools >Scheduler***.
   - » The **Scheduler** screen appears.

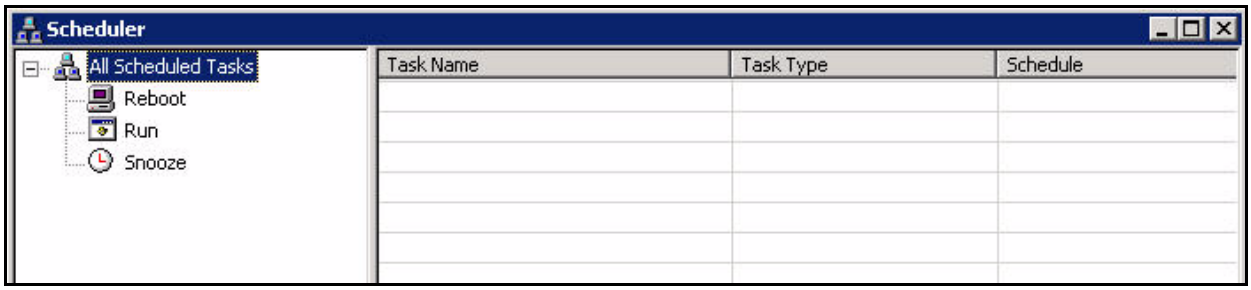


Figure 68: Scheduler screen

2. Right-click **Snooze** and select **Add New Task**.

» The **Please Provide Information about the Snooze** dialog box displays.

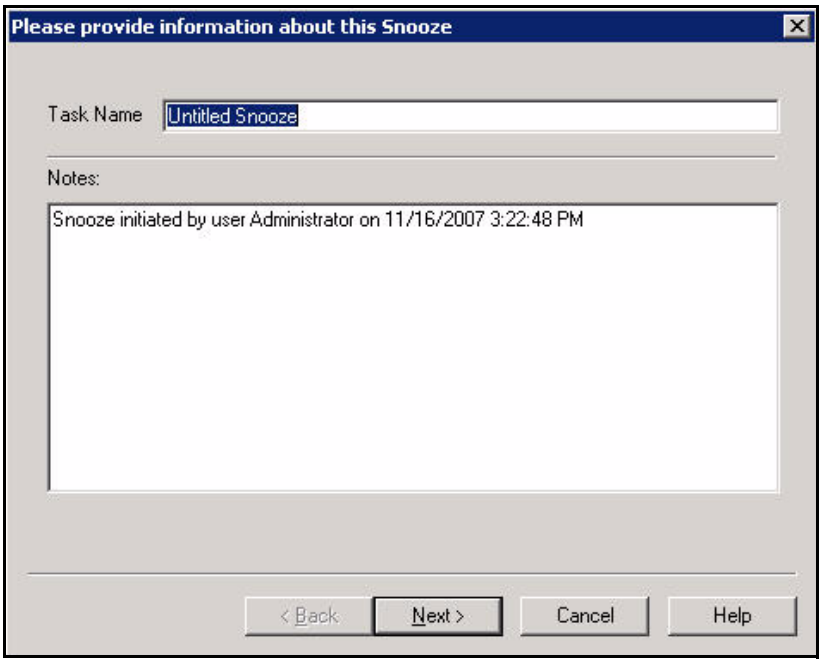


Figure 69: Please provide information about this Snooze dialog box

3. Enter **Snooze Task** name in the **Task Name** field.
4. Add notes regarding why the snooze is taking place in the **Notes** section of this screen.
5. Click the **Next** button.

» The **Please select computer(s) to Snooze** screen displays.

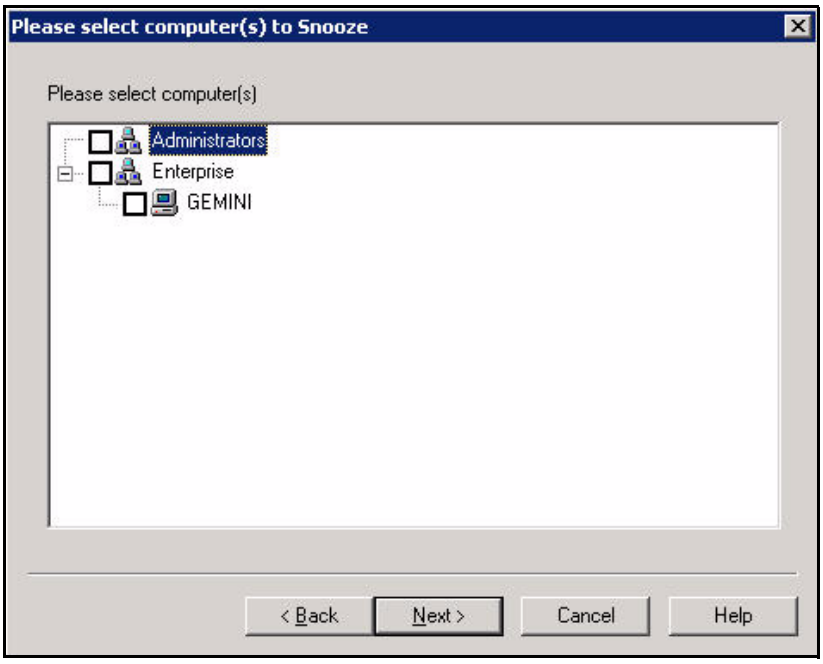


Figure 70: Please select computer(s) to Snooze screen

6. Select the **checkbox** in front of any group of computers (or expand the trees as desired) and select one or more computers that you would like to snooze.
7. Click the **Next** button.
   - » The **Snooze Schedule** screen displays.

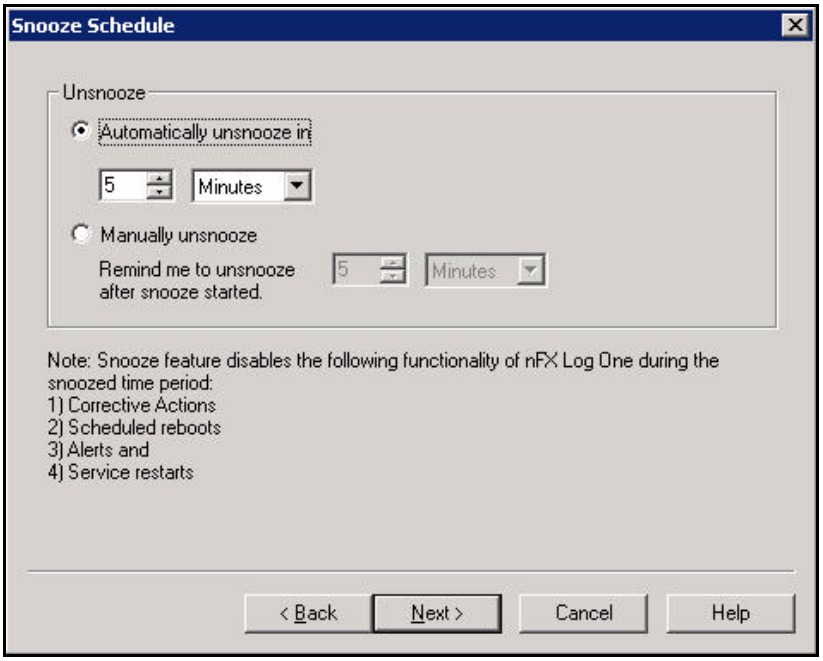


Figure 71: Snooze Schedule screen

8. Select the **Automatically unsnooze in** radio button if you want the snooze to be disabled automatically, according to a timeframe you set. Or, select the **Manually unsnooze** radio button if you want to disable the snooze manually.

Important

If you would like to un-snooze the system manually, instructions are provided in the next section.

9. Click the **Next** button.

» The **Please provide information about this Snooze** screen displays.

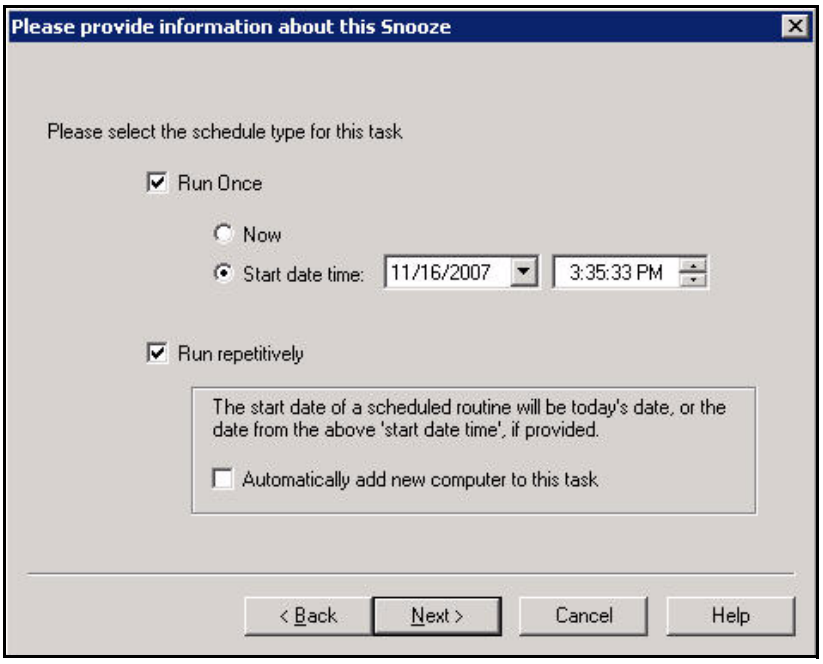


Figure 72: Please provide information about this Snooze screen

10. To run the Snooze just once, check the **Run Once** checkbox. To run on a schedule, click **Run repetitively** checkbox. One, the other or both may be checked.
11. Select the **Now** radio button if you want the **Snooze** to take effect immediately. Or, select the **Start date time** radio button if you want to delay the snooze to a specific date and time.
12. Check the **Automatically add new computers to this task** if desired.
13. Click **Next**.

» The **Snooze Schedule** screen appears.

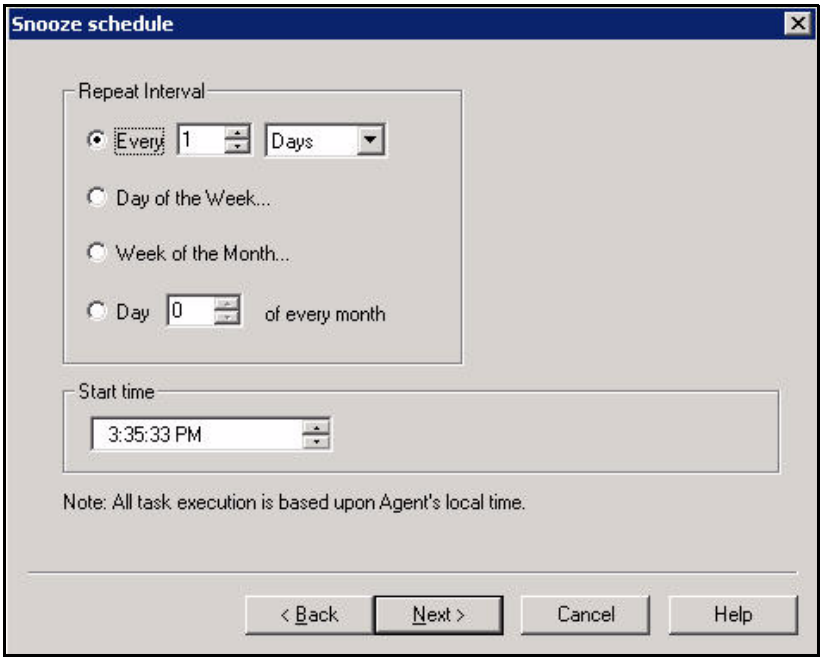


Figure 73: Snooze schedule screen

14. Select the desired **Repeat Interval** and **Start time** for the Snooze Schedule.
15. Click **Next**.
    - » The **Summary** screen will appear.
16. Click the **Back** button to make any changes.
17. Click the **Finish** button to complete your snooze configuration.

To UnSnooze a System

After the designated time period in the **Snooze Computer for a duration of time** field has expired, the **Snooze Reminder** screen displays.

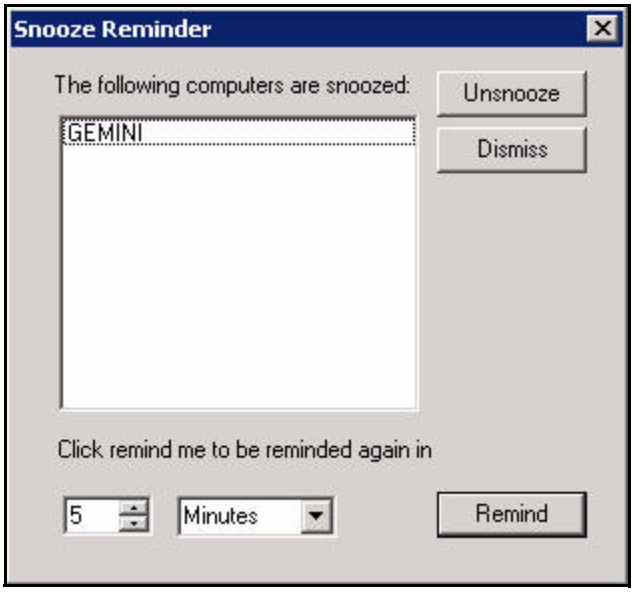


Figure 74: Snooze Reminder screen

There are several options.

1. To **unsnooze the system** immediately, click the **UnSnooze** button.
2. To **extend the Snooze duration**, set the time period and click the **Remind** button.
3. To **cancel the snooze**, click the **Dismiss** button.

Changing the Properties of a Scheduled Snooze

Once a Snooze has been scheduled to occur on a regular basis, you can access the **Snooze properties** by following the steps below.

1. From the nFX Log One Console menu, select ***Tools> Scheduler.***
   - » The **Scheduler** screen appears.
2. Highlight **Snooze** on the left pane.
   - » A list of all scheduled Snoozes displays.

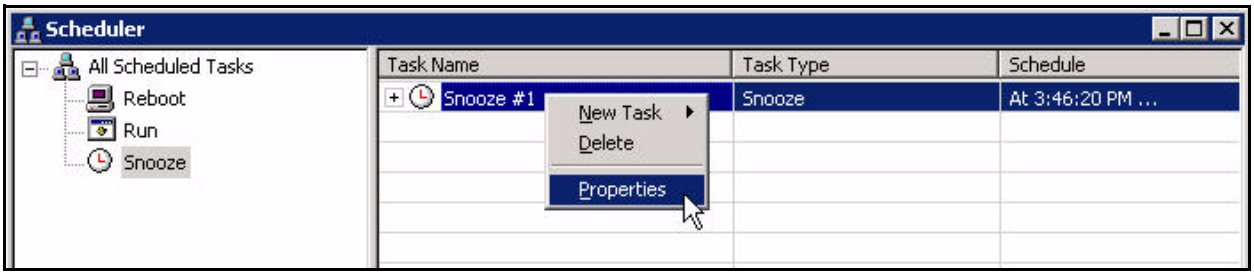


Figure 75: Scheduler Right-click menu

3. Right click on any **Snooze**.
4. Select **Properties** to view or edit the properties of the snooze. See Step » in "Configuring a Snooze" on page 79.
5. If changes are made, click **Next** until done. Then, click **Finish**.

Reboot Tool

To keep your servers running smoothly, it may be necessary to reboot them for various reasons. For example, some applications consume excess resources due to memory leaks and over time could cause the system to function below acceptable limits - unless it is regularly rebooted. nFX Log One allows you to automate the process of rebooting the systems by allowing you to reboot a remote system without leaving your desktop, or configure a reboot schedule for multiple systems.

1. From the nFX Log One Console menu, select ***Tools >Scheduler.***
   - » The **Scheduler** screen appears.

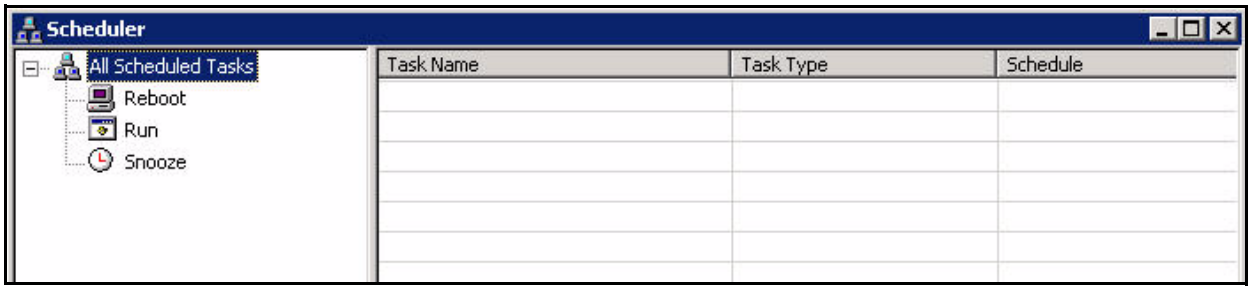


Figure 76: Scheduler screen

2. Right-click **Reboot** and select **Add New Task**.
   - » The **Please Provide Information about the Reboot** dialog box displays.

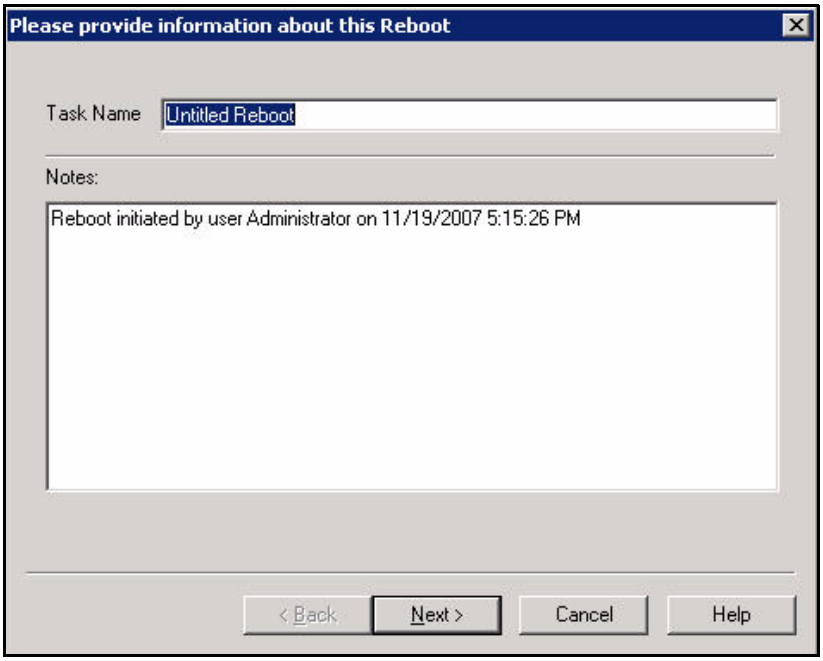


Figure 77: Please provide information about this Reboot screen

3. Enter a **Reboot Task Name** in the **Task Name** field.
4. Enter any descriptive information about the reason for the reboot in the **Notes** section of this screen.
5. Click the **Next** button.

» The **Please select computer(s) to Reboot** screen displays.

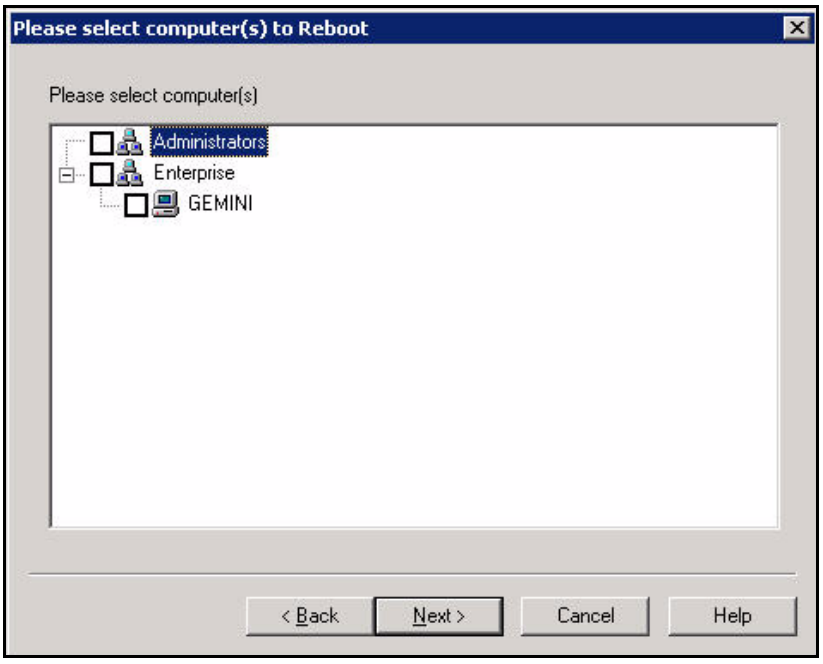


Figure 78: Please select computer(s) to Reboot screen

6. Select the **checkbox** next to the group of computers that you want to reboot, or expand the tree and click on one or more computers that you want to reboot.
7. Click the **Next** button.

» The **Reboot Schedule** screen displays.

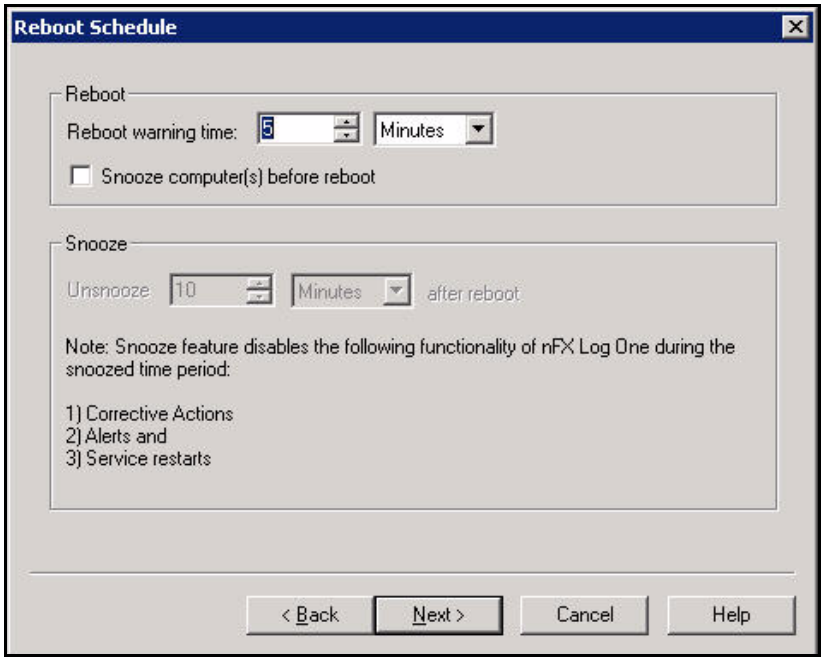


Figure 79: Reboot Schedule screen

8. Select a **Warning Time** from the **Reboot warning time** pull-down menu to identify how many minutes prior to the upcoming reboot that you would like nFX Log One to send out a **Warning Message**.

Important

It is ***strongly*** advisable that you **Snooze** the machine during a planned reboot to prevent any false alerting from occurring.

9. Click the **Next** button.
10. The **Please provide information about this Reboot** screen displays.

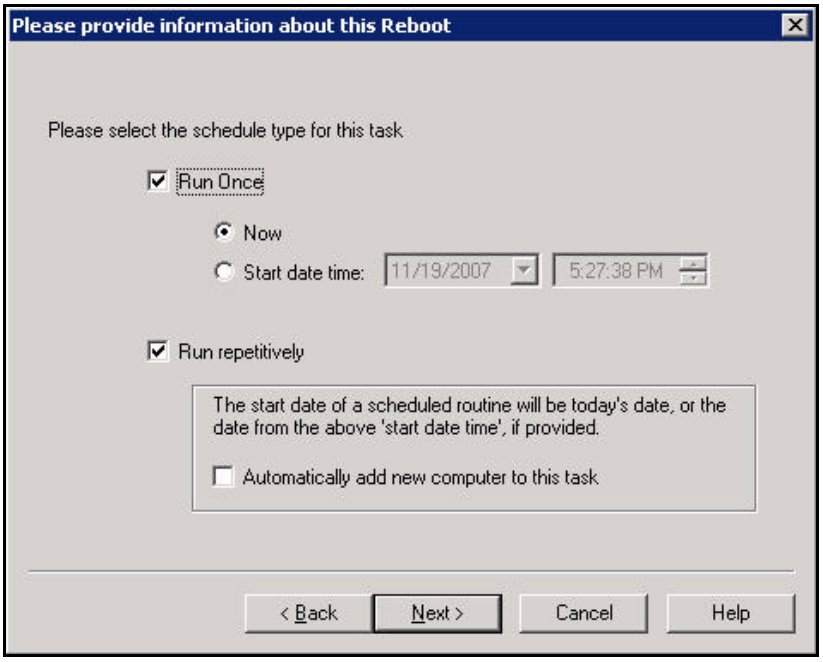


Figure 80: Please provide information about this Reboot screen

11. To run the **Reboot only one time**, check the **Run Once** checkbox. Then decide whether to Reboot Now or at a set date and time.
    a. To perform the **Reboot** now, click the **Now** radio button.
    b. To perform the **Reboot** later, click the **Start date time:** radio button and select the **date** and **time** for the reboot.
12. To run the **Reboot on a schedule**, check the **Run repetitively** checkbox. Set the date and time the next screen.
13. Click the **Next** button.
    » The **Reboot schedule** screen displays.

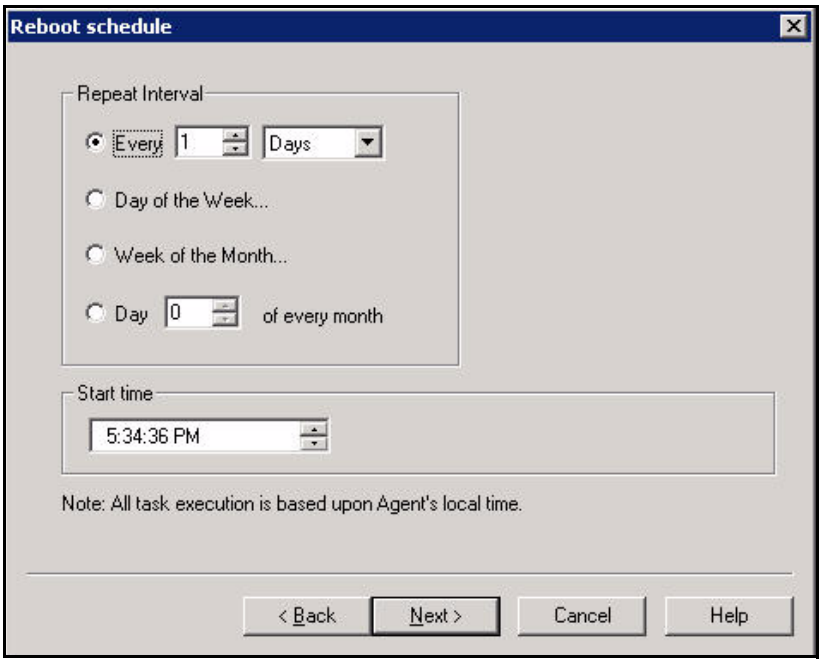


Figure 81: Reboot Schedule screen

14. Set the desired **Repeat Interval** and **Start time** for the Reboot Schedule.
15. Click the **Next** button.
16. After setting your reboot schedule, a **Summary** screen displays.
17. Click the **Back** button to make changes.
18. Click the **Finish** button to complete your **Reboot** configuration.

Changing the Properties of a Scheduled Reboot

Once a Reboot has been scheduled to occur on a regular basis, you can access the **Reboot Properties** by following the steps:

1. From the nFX Log One Console, select ***Tools> Scheduler***.
   - » The **Scheduler** screen appears.
2. Highlight **Reboot** on the left pane.
   - » A list of all scheduled Reboots display.
3. To view or edit the **Reboot Properties**, **Right-click** on any **Reboot**.
4. Select the **Properties**.
5. If changes are made, click **Next** until done. Then, click **Finish**.

Run Tool

nFX Log One's Run Tool allows you to automate the running of an executable on any computer or group of computers where the nFX Log One Agent software has been deployed. An executable can be run once or according to user-definable schedule.

To automate the running of an executable, follow these steps:

1. From the nFX Log One Console menu, select ***Tools > Scheduler***.
   - » The **Scheduler** screen appears.

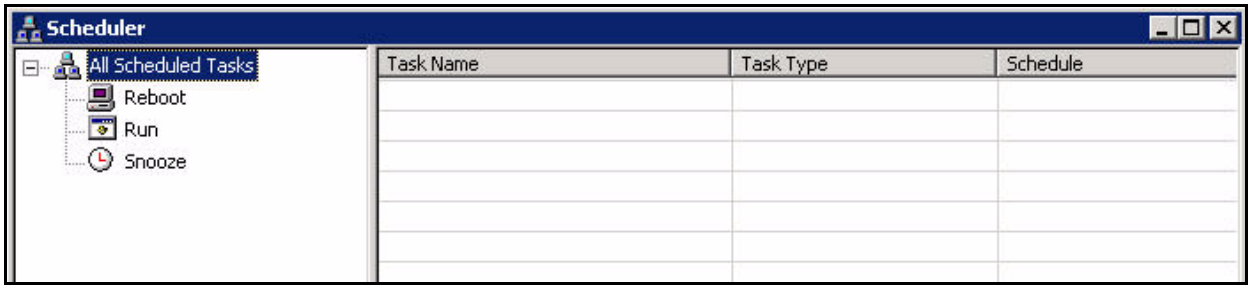


Figure 82: Scheduler screen

2. Right-click **Run** and select **Add New Task**.
   - » The **Please provide information about the Run Task** screen displays.

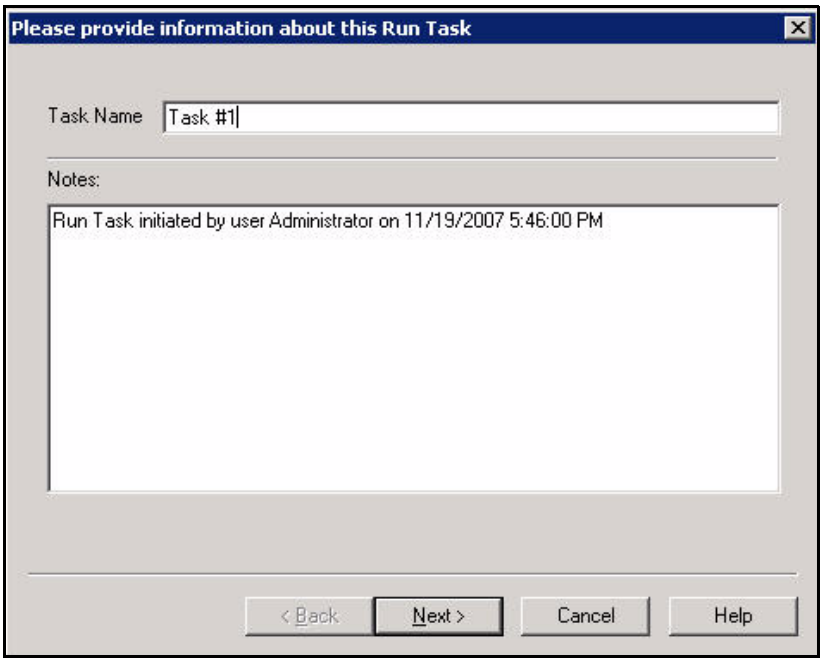


Figure 83: Please provide information about the Run Task screen

3. Enter the Run Task Name in the **Task Name** field.
4. Enter Run Task information in the **Notes** section.
5. Click the **Next** button.
   - » The **Please select computer(s) to Run Task** screen displays.

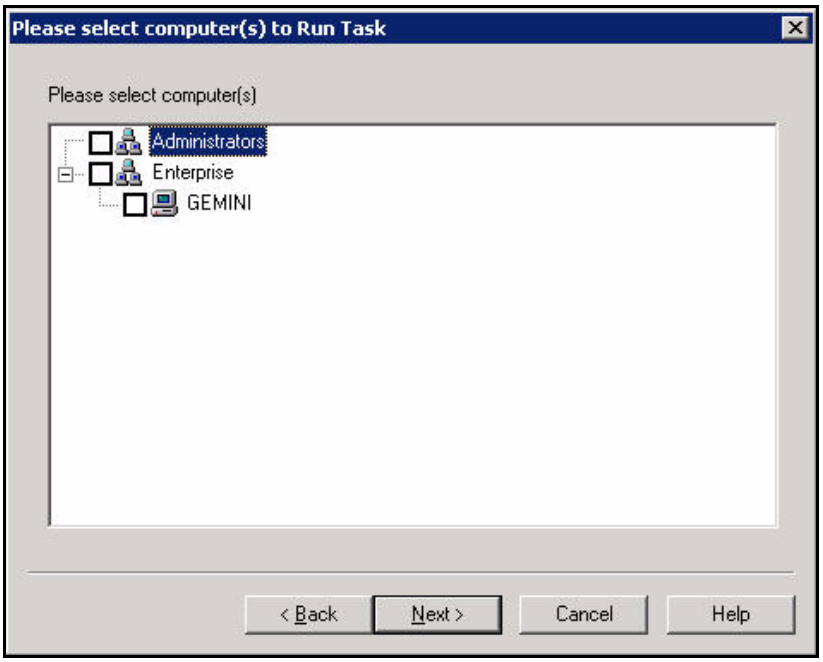


Figure 84: Please select computer(s) to Run Task screen

6. Select the checkbox next to the group of computers that you want to run an executable on, or expand the tree and click on one or more multiple computers. If you choose to run the same executable on multiple machines, the executable must be found in the same path on each computer you have specified.
7. Click the **Next** button.
   - » The **Run Task Options** screen displays.

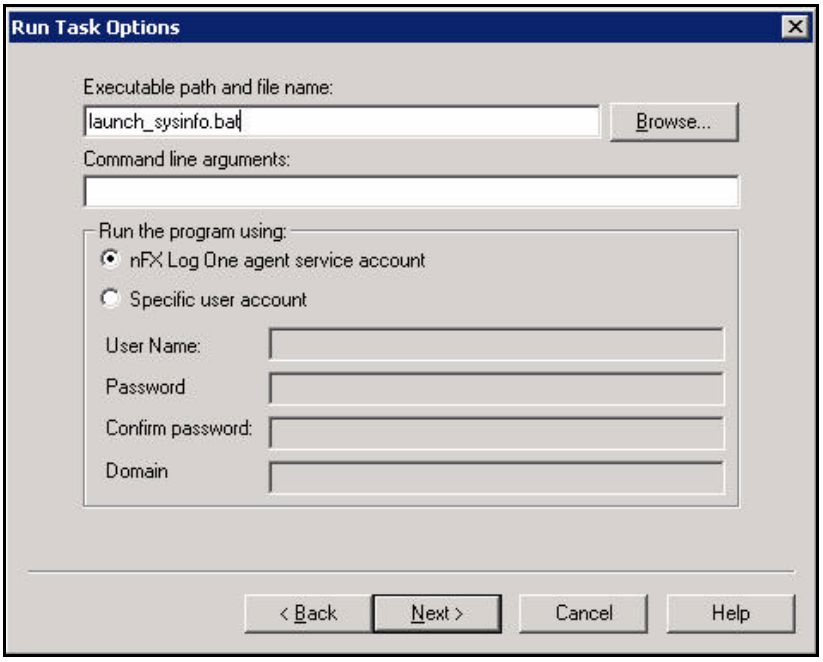


Figure 85: Run Task Options screen

8. Enter the complete path to the file name of the executable that you want to run in the Executable Path and File Name field. (You can use the Browse button if necessary).
9. Fill out the rest of this screen.

Important

Keep in mind that the *specified* **User Account** *must have* permissions to run the executable on each desired system.

10. Click the **Next** button.
    - » The **Please provide information about this Run Task** screen displays.

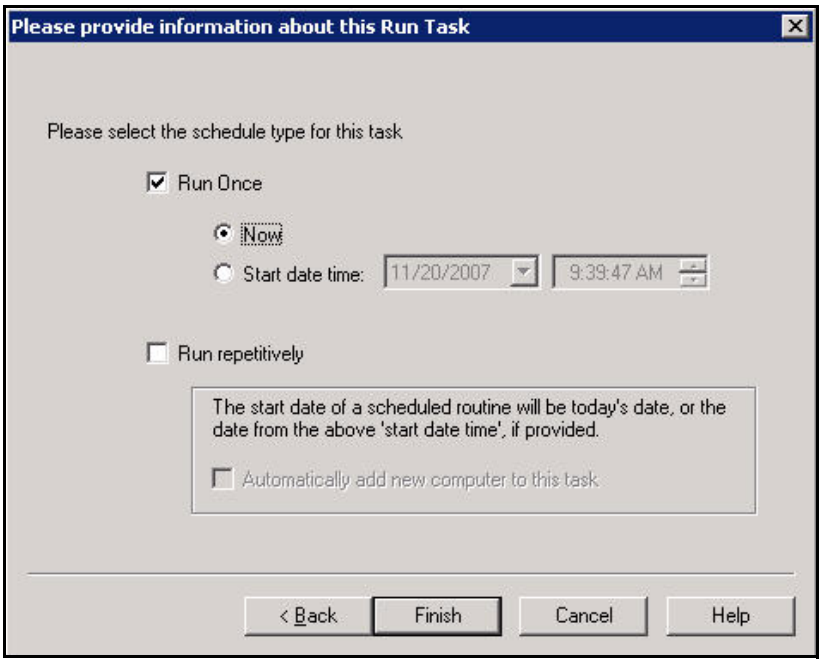


Figure 86: Please provide information about this Run Task screen

11. To run the Task just once, check the **Run Once** checkbox. To run the task on a schedule, click **Run repetitively** checkbox. One, the other or both may be checked.
12. Select the **Now** radio button if you want the **Task** to run immediately. Or, select the **Start date and time** radio button if you want to delay the running of the task to a specific date and time.
13. Check the **Automatically add new computers to this task** if desired.
14. Click the **Next** button.
    - » The **Run Task schedule** screen displays.

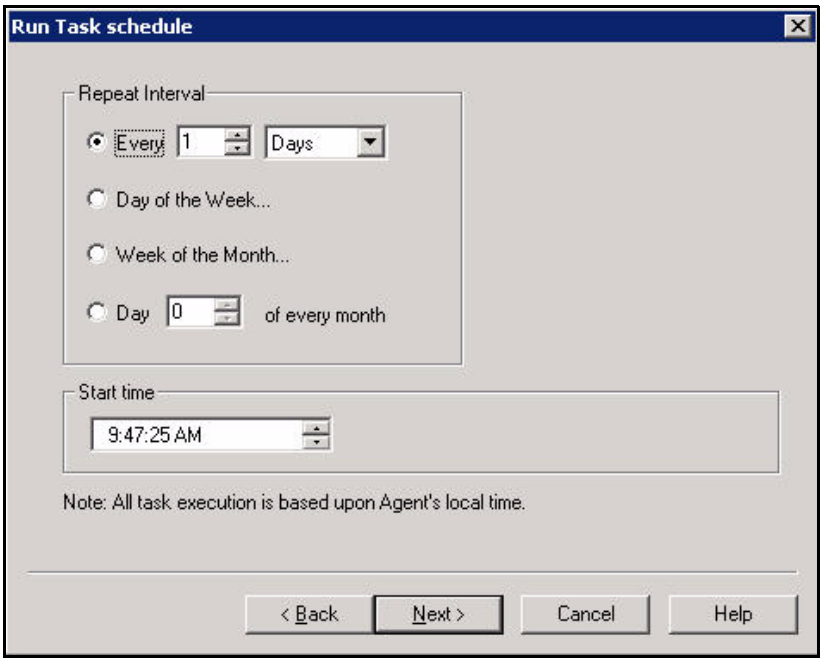


Figure 87: Run Task schedule screen

15. Select the desired **Repeat Interval** and **Start time** for the **Task**.
16. Click **Next**. The **Summary** screen appears.
17. Click the **Back** button to make changes.
18. Click the **Finish** button to complete your **Task** configuration.

Changing the Properties of a Scheduled Task

Once an executable has been scheduled to occur on a regular basis, you can access the **Run Task** properties using the **Scheduler**.

1. From the nFX Log One Console menu, select ***Tools > Scheduler***.
   - » The **Scheduler** screen appears.
2. Highlight **Run** on the left pane and a list of all scheduled tasks displays.
3. **Right-click** on any task and select **Properties** to view or edit the properties of the task.
4. If changes are made, click **Next** until done. Then, click **Finish**.

Scheduler

nFX Log One's **Scheduler** tool provides you with single screen access to all scheduled reboots, reports, snoozes, and task runs. You can access the **Scheduler** option by selecting ***Tools> Scheduler*** from the nFX Log One Console menu. The **Scheduler** tool provides you with the following information regarding each scheduled event: **Task name**, **Task type**, **Schedule**, **Creator**, **Task status**, **Last result**, **Next run time**, and **Last run time**.

Using the Scheduler

1. Access the Schedule from the nFX Log One Console menu, ***Tools > Scheduler***.

   » The **Scheduler** screen appears.

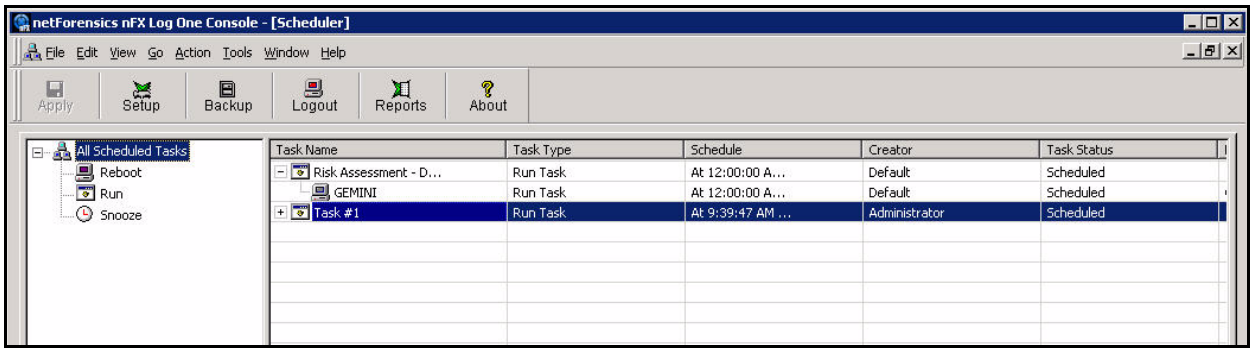


Figure 88: Scheduler screen

2. To schedule a new **reboot**, **report**, **snooze**, or **task run**, simply **Right-click** on the appropriate task type on the left pane of the Scheduler screen and follow the screen-by-screen instructions.

Service Control Manager

With the nFX Log One **Service Control Manager**, you can control any remote or local service on any system where an nFX Log One Agent resides. This convenient feature allows you to start, restart, or stop services on a remote machine without leaving your management workstation. To access the Service Control Manager, follow these steps.

1. From the nFX Log One Console menu, select ***Tools > Service Manager***.

   » The **Services Control** screen displays.

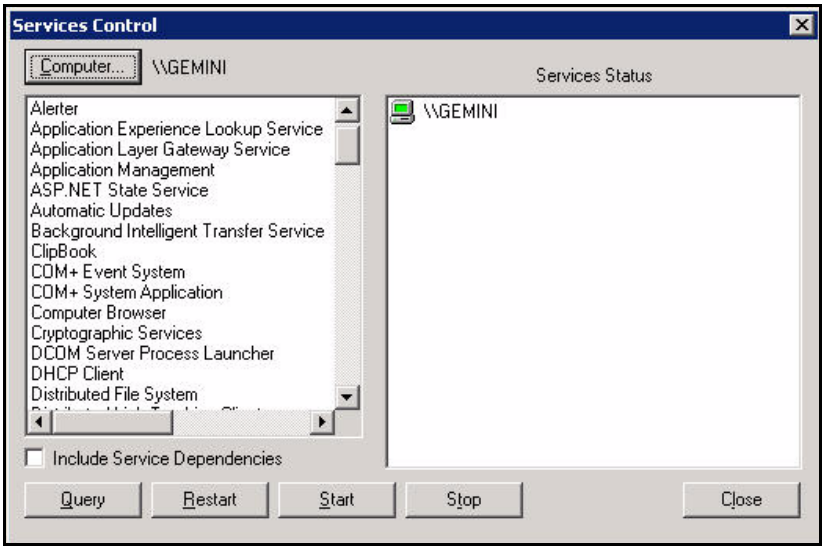


Figure 89: Service Control screen

2. Click the **Computer** button to select the desired computer.
3. **Highlight** the computer.
4. Click the **OK** button.

5. Click the **desired service(s)**. Multiple services can be selected by holding the **CTRL** and **SHIFT** keys.

Important

If you would like to include any dependent services in the action you select, you must check the **Include Service Dependencies** checkbox. This option is *NOT* selected by default.

6. Click the **Query** button to determine the current status of the selected services. Each selected service will appear in the Services Status pane with one of the following icons:

Indicates that the service is currently **started**

Indicates that the service is currently **stopped**

Indicates that the service is currently **disabled**

7. One of the following actions can be taken by using the buttons on the bottom of the screen:
   - **Restart** - stops the selected service(s) and then starts the selected service(s).
   - **Stop** - stops the selected service(s).
   - **Start** - starts the selected service(s).

Alert Maintenance Tool

The **Alert Maintenance** tool provides a way to stop notifications from being delivered to their destination. If there are a number of pending unnecessary pages, removing the **Alerts** can be helpful.

1. From the nFX Log One Console menu, select ***Tools > Alerting Maintenance***.
   » The **Alerting Maintenance** screen displays.

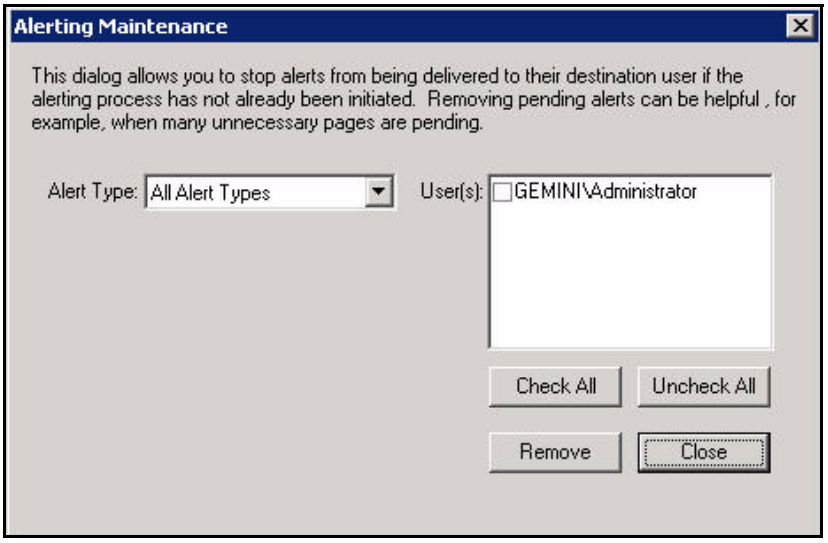


Figure 90: Alerting Maintenance screen

2. From the **Alert Type** drop-down menu, select the type of alert that needs to be removed. If all alerts need to be removed for a certain **user ID** the **All Alert Types** option can be selected.
3. **Check** each **User ID** that requires the **Alert Type** to be removed. Valid users of nFX Log One are listed in the **User(s)** list. The **Check All** button allows for all users' notifications to be removed from the database table **ALERTSTBL**.
4. Once all parameters have been designated, click the **Remove** button.
   » A 'Delete Alert Confirmation' screen displays.

5. Select **Yes** to continue.

Database Configuration Tool

nFX Log One's **Database Configuration** tool enables you to direct nFX Log One to a new database for data storage. Currently, nFX Log One supports either Microsoft's SQL Desktop Edition (MSDE) or Microsoft SQL Server 2000 as its engine for data management.

Important

After installation, you can use the **Database Configuration Tool** to direct nFX Log One to a new database.

Important

If you change nFX Log One's default database, you may also need to change the **data quota management** settings associated with the database. You can use the **Database Quota Management Tool** to adjust these settings.

Changing Database Repositories

1. From the nFX Log One Console menu, select ***Tools> Database Configuration***.
   - » The **Database Settings** screen displays, showing your current settings.

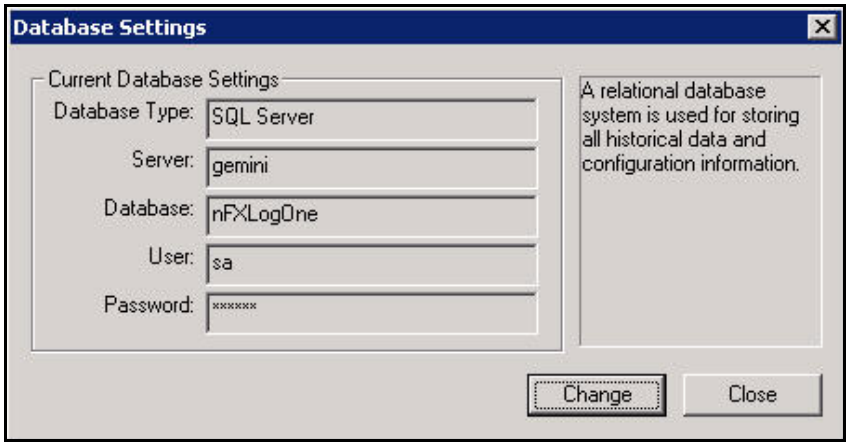


Figure 91: Database Settings screen

2. To change the database settings, click the **Change** button.
   - » The **Database Migration** screen displays with a warning stating that during migration only your configuration data will be migrated to the new database.

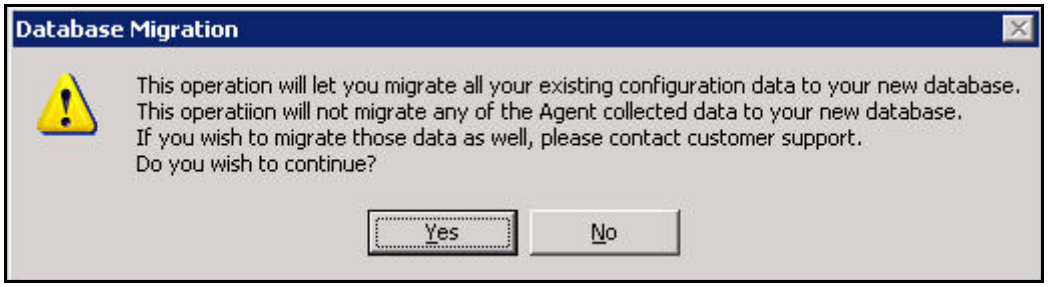


Figure 92: Database Migration screen

Warning

If you want to *migrate one* or *all* **nFX Log One Agent-collected data**, ***you must speak with netForensics Technical Support*** before proceeding.

3. Click the **Yes** button.
   - » The **Database Settings Wizard** screen displays.

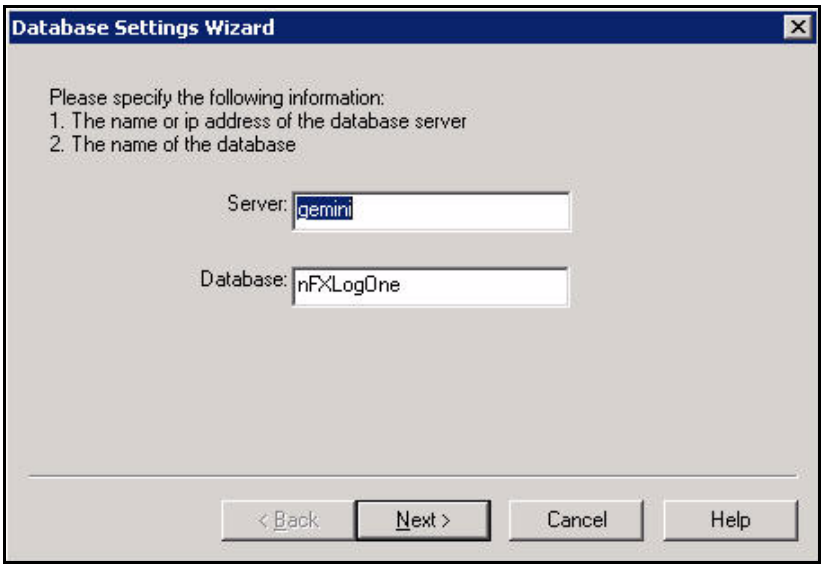


Figure 93: Database Settings Wizard screen

4. Enter the **Name** or **IP address** of the **Database Server** in the **Server** and/or **Database** fields.
5. Click the **Next** button.
6. Enter the **User** Name and **Password** for nFX Log One to use to authenticate itself to the database.
7. Click the **Finish** button.

Important

When you click the **Finish** button at the completion of the **Database Settings Wizard**, a database connection will attempt to verify the information supplied throughout the Wizard, and you will be notified of a successful connection. You will also receive a second notification when all data has been successfully migrated by the Wizard.

Database Quota Management Tool

The **Database Quota Management** tool enables the nFX Log One Administrator to define how long historical data will be held on the hard disk of the nFX Log One Management Server storing the nFX Log One Database Repository.

1. From the nFX Log One Console menu, select ***Tools > Database Quota Configuration***.
   - » The **Database Quota Management Settings** screen displays.

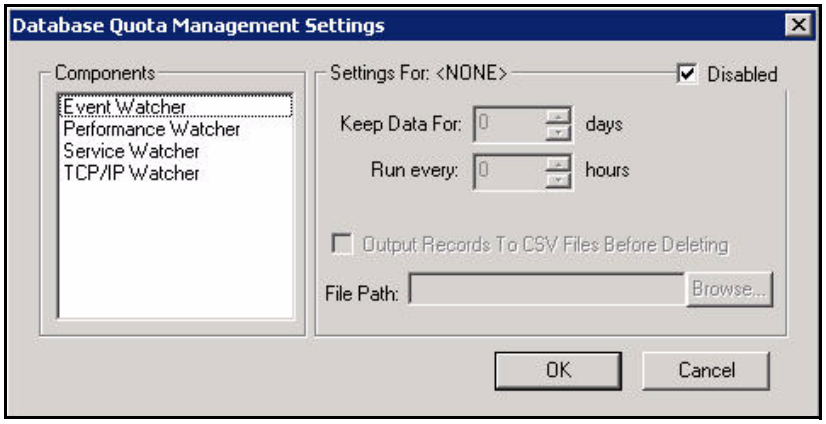


Figure 94: Database Quota Management Settings screen

2. To change the **quota management** based upon the different components, **highlight** a **Component** under the **Components** section.
3. The **Settings For: <component name>** section designates how long the historical data will be held on the hard disk for that component. Click the **Disabled** checkbox (so that it is deselected) and enter the desired information.
4. The **Keep Data For** option allows you to select the amount of days before the data will be deleted.
5. The **Run every** option allows you to choose how often the hard disk will be scanned.
6. The **Output Records to CSV Files Before Deleting** option tells nFX Log One to generate a CSV file before deleting all of the data from the hard disk. Enter the path for the CSV file.
7. Click **OK**.

Backup and Restore Tool

The **Backup** tool is used to backup all of the nFX Log One Configuration Files found in the nFX Log One directory. This configuration information can be restored to the same system or any other system that has had its configuration deleted or corrupted by using the **Restore** tool.

Backing Up an nFX Log One Configuration

It is recommended that the nFX Log One Configuration Files be backed up each time that you make a change to your nFX Log One configuration.

To back up an nFX Log One configuration:

1. Click the **Backup** icon on the nFX Log One toolbar or select ***File > Backup*** from the nFX Log One Console menu.

   » The **Backup Restore** screen displays.

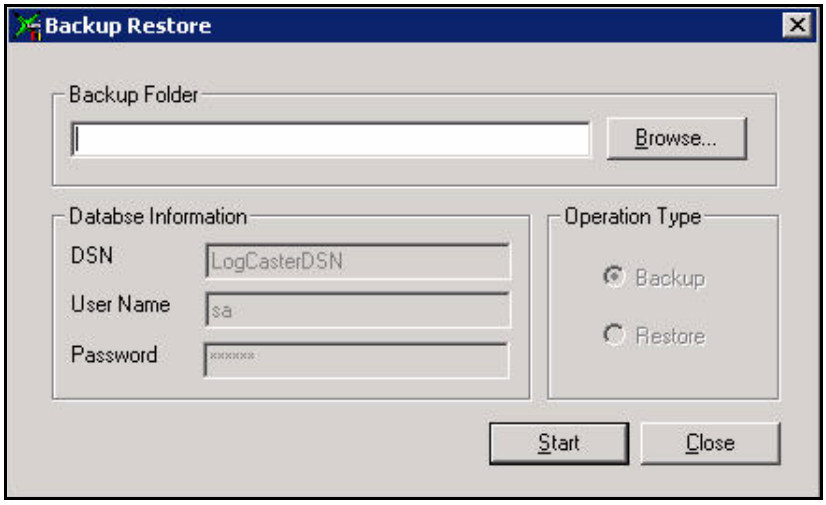


Figure 95: Backup Restore screen

2. **Choose** or **confirm** a file destination where you would like the backup configuration to be stored.

   It is recommended that a separate folder be set up for your backup files on another system other than the nFX Log One Server.

3. Click **Start** when ready to perform the Backup.

Restoring an nFX Log One Configuration

The **Restore** tool is used to restore all of the nFX Log One Configuration Files on the same system or another system whose configuration may have been lost, deleted, or corrupted. This eliminates the need to reconfigure nFX Log One on your system after any disaster.

To restore an nFX Log One configuration:

1. Click the **Backup** icon on the nFX Log One toolbar, or select ***File > Restore*** from the nFX Log One Console menu.

   » The **Backup Restore** screen displays

2. You may be prompted to close all nFX Log One Configuration screens, and select the file location of your nFX Log One backup.

Important

During a restoration to an nFX Log One Server you must ensure that the computer name used for the nFX Log One Server and all Agents have the same name as when the configuration files were backed up.

Utilizing Reports in netForensics Reporting

This section will provide you with the information that you'll need to get the most out of your **netForensics Reporting** software. The section covers the following topics:

- Report Execution
- Exporting Reports
- Message Text Searching

Report Execution

The default **netForensics Reporting** home page displays Report folders based on Report Groups as well as additional Security Report folders, which contain relevant canned reports.

To access reports, follow these steps:

1. To access the netForensics **Report Manager** from the **Windows** menu, select ***Start > All Programs > netforensics> Reporting > Report Manager.***

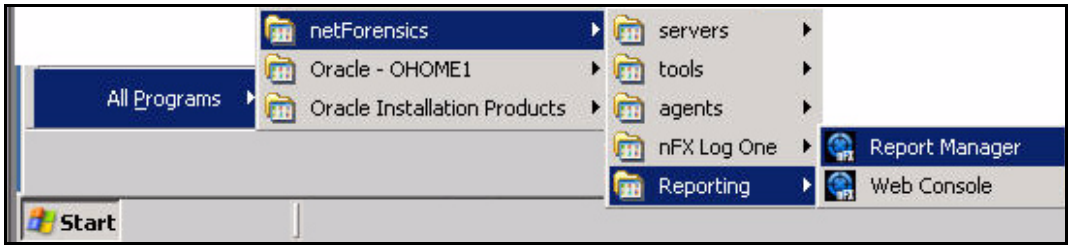


Figure 96: Access Report Manager from Windows menu

» The **SQL Server Reporting Services Home page** appears.

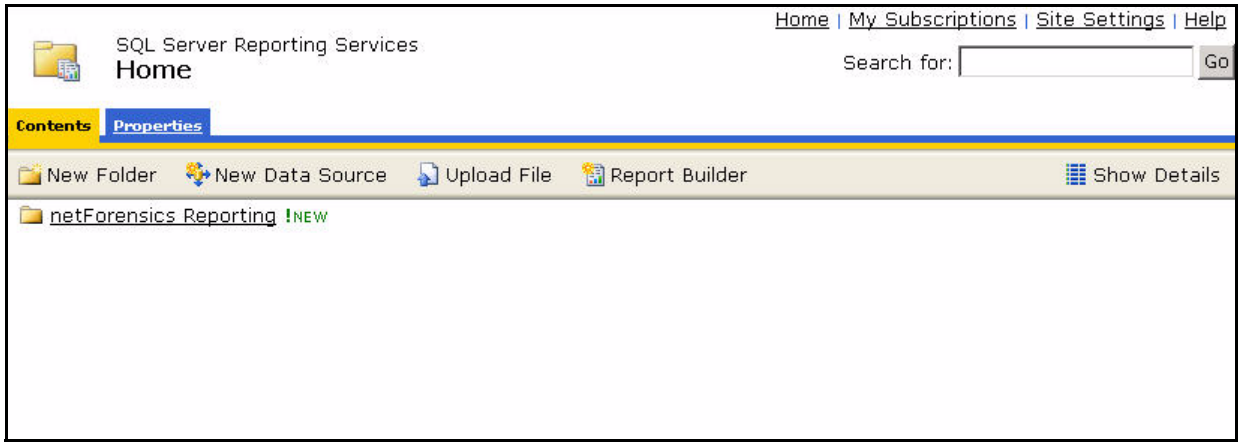


Figure 97: SQL Server Reporting Services screen

2. Click the **netForensics Reporting** link.

» The **Report Manager contents** web page displays listing the Report sub-folders based on Report groups.

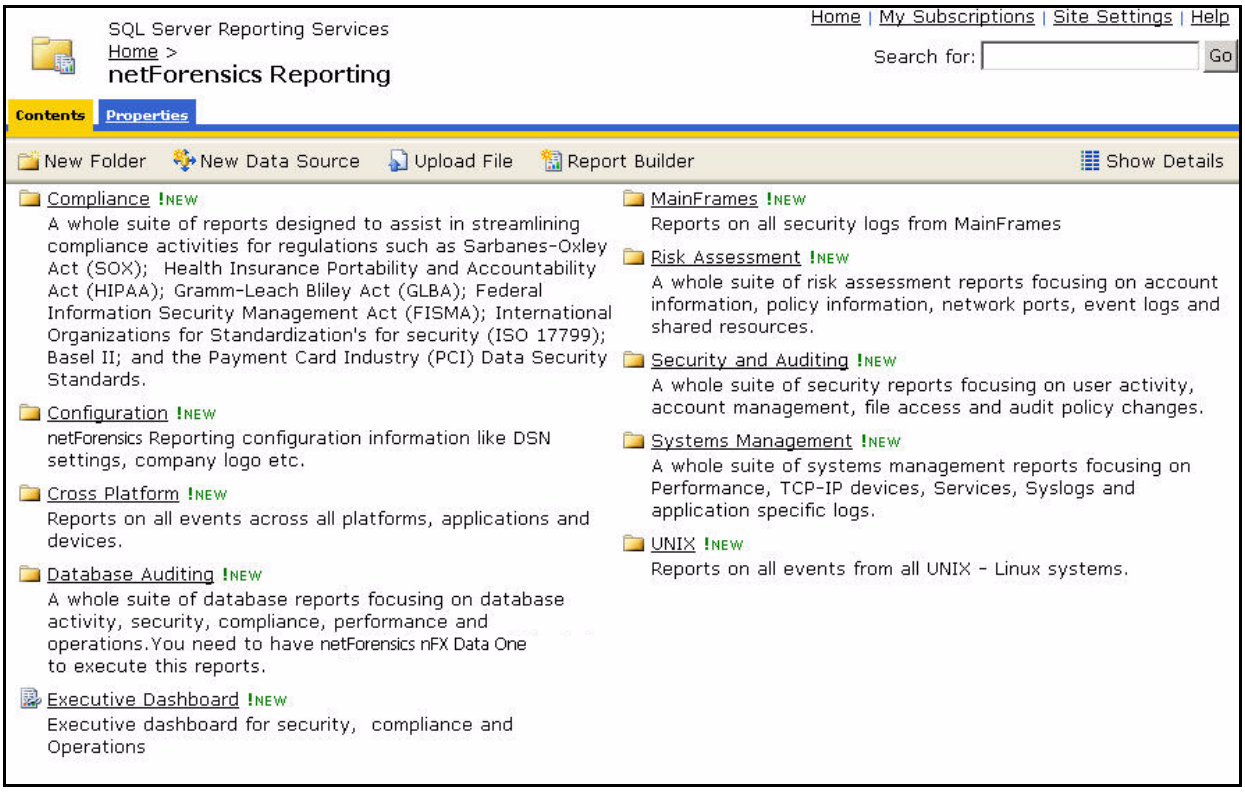


Figure 98: netForensics Reporting Home page (Report Manager)

3. From the **Report Manager** screen, select a specific **Report Type** from the displayed list of Reports.

» For example: if the **Security and Auditing** link is clicked, the following screen displays:

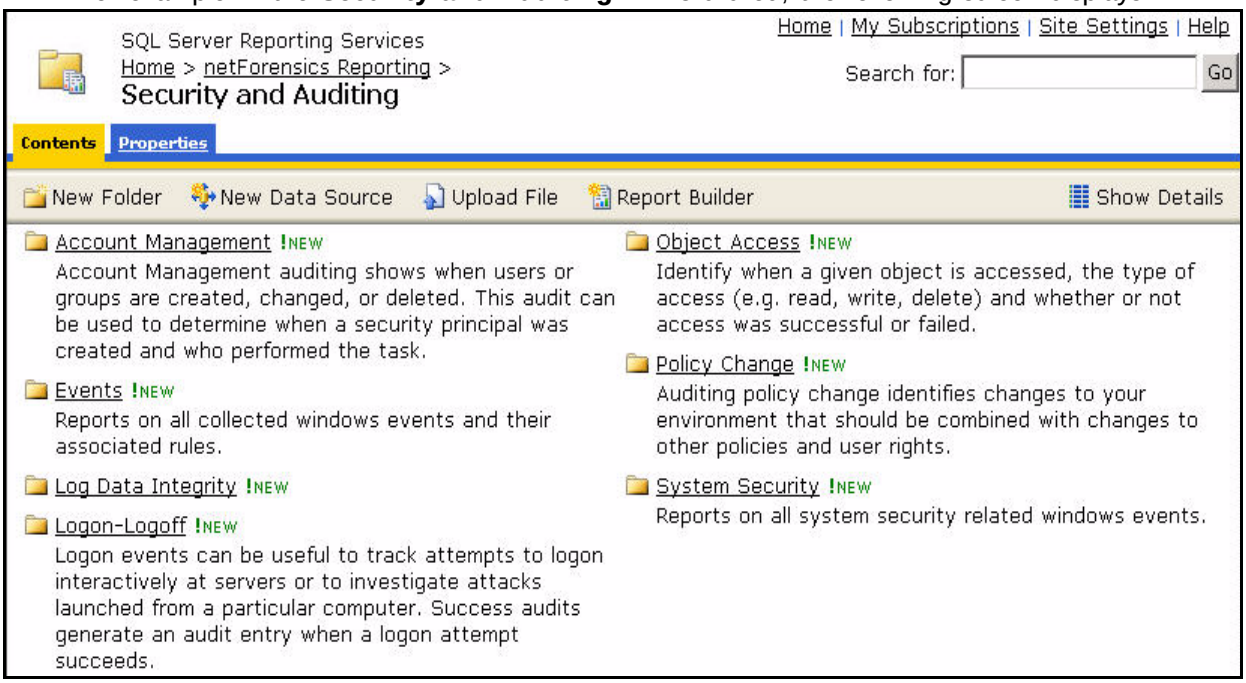


Figure 99: SQL Server Reporting Services Security and Auditing Reports Page

4. Select the **Report** that you want to use. For example: click the **Account Management** link.

   » The **Account Management** reports page appears.

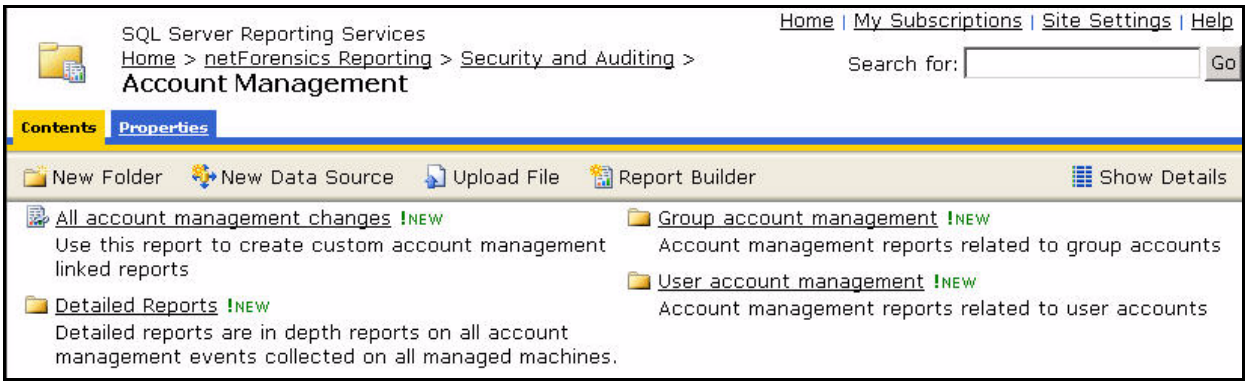


Figure 100: Account Management Reports page

5. Click the **All account management changes** report link.

   » The **All Accounts Management Changes configuration** screen appears.

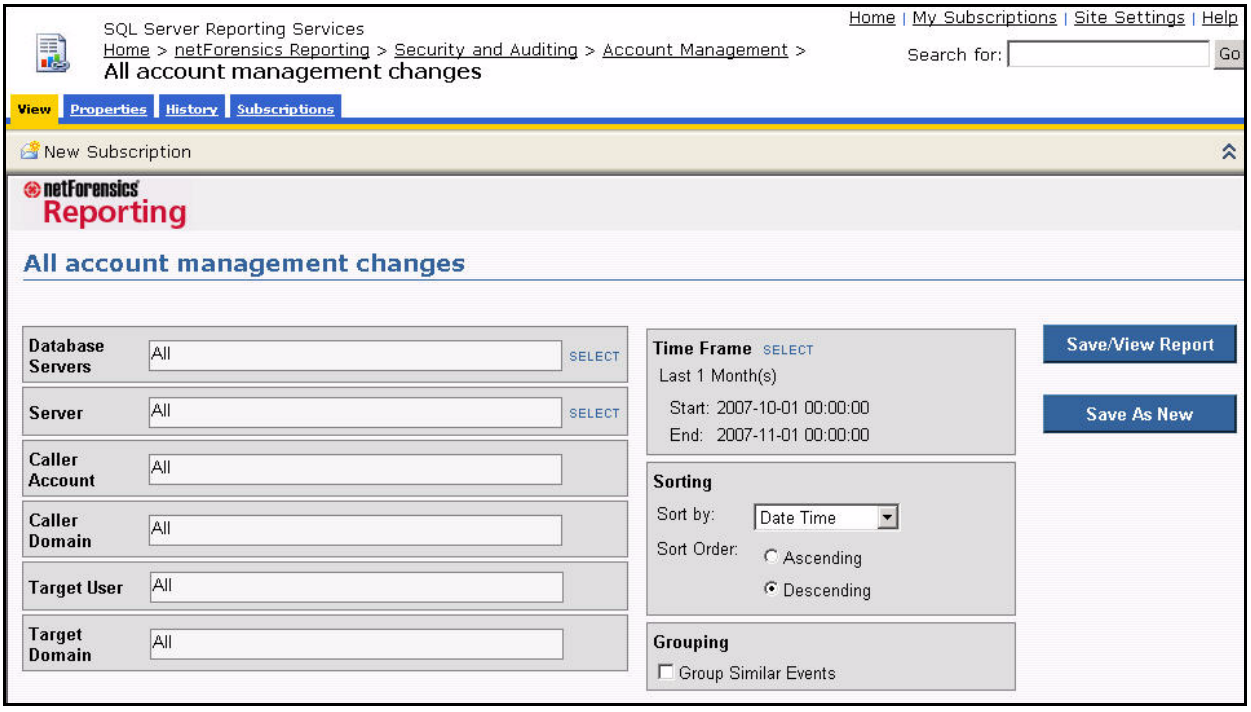


Figure 101: All Accounts Management changes screen

6. **Verify / modify** the Report's parameters and click the **Save / View Report** button to execute the report.

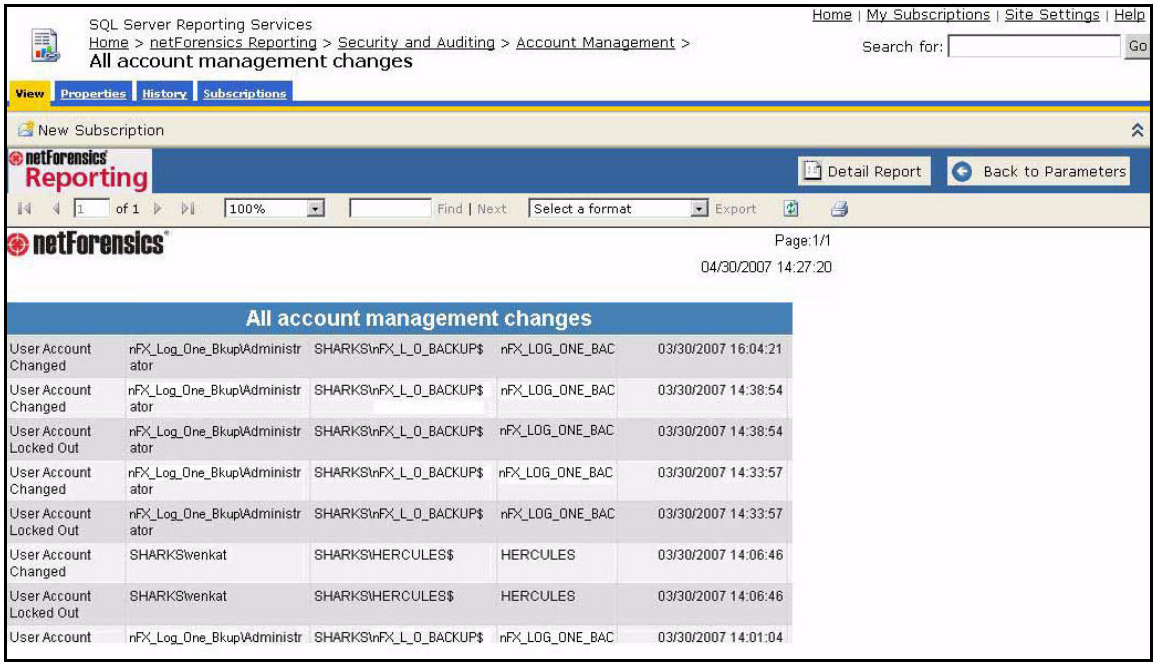


Figure 102: All Account Management Changes Report

7. Check the Report to determine if the parameters for the Report need to be adjusted.

Exporting Reports

In **netForensics Reporting**, you can easily **export a Report** from the **Report Manager**. The steps below will show you how to complete this task:

1. Click on the **Select a format** menu drop-down after you have executed a report such as the one listed above.
   - » A list of various **Export Formats** displays.

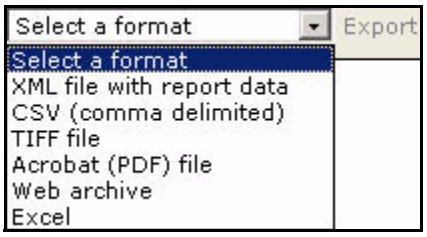


Figure 103: Exports menu

2. Select the **Export Format** that you want to use.
3. Click on the **Export** link directly to the right of the drop-down menu.
   - » The Report is displayed in a new window.

Important

The **Report Toolbar** (shown above) is part of the **HTML Viewer**. When you click the **Export** link, the **Report** opens in a new browser window, in a viewer that *supports* the **Export Format** that you've selected.
For example: If you selected TIFF as the **Export Format**, your report would display in a viewer that supports TIFF file types.

Message Text Searching

netForensics Reporting allows you to *add* **Search Criteria** for the Report that you are planning to run. The steps below will show you how to complete this task:

1. Go to the **Report** that you are planning to run.
2. Select the **Select link** in the **Message Text Searching** section of your Report.
   - » The **Message Text Search - Web Page Dialogue** screen displays.



Figure 104: Message Text Search - Web Page Dialog screen

3. Select the **Search Criteria** that you want to add and click on the **Add** button.
4. Once you have added all of your Search Criteria, click the **OK** button.
   - » Your Search Criteria has been added.

Report Configuration

In this section, you will learn about the various operations that can be performed on reports and folders including the following:

- Saving Reports
- Moving Reports
- Deleting Reports
- Changing Company Logos in a Report
- Changing the Data Source DSN settings
- Report History
- Report Subscription
- Report Access and Role Assignments

Saving Reports

Once you have executed the Report that you want to use, you can alternatively make a copy of the report using the **Save As New** option. This is recommended if you would like to preserve the default canned reports.

1. Run the report as desired.
2. Click on the **Save As New** button.
   - » The Report is saved in the currently opened folder.

Moving Reports

There may be times when you may want to *move* a Report from one location to another. The steps below will show you how to complete this task:

Important



It is recommended to create a custom folder at the root of **netForensics Reporting** that can be used to hold all custom reports.

1. In **Report Manager**, open the folder that contains the Report that you would like to move.
2. Click on **Properties** tab.
   - » The **Report Manager Report Properties** screen appears.

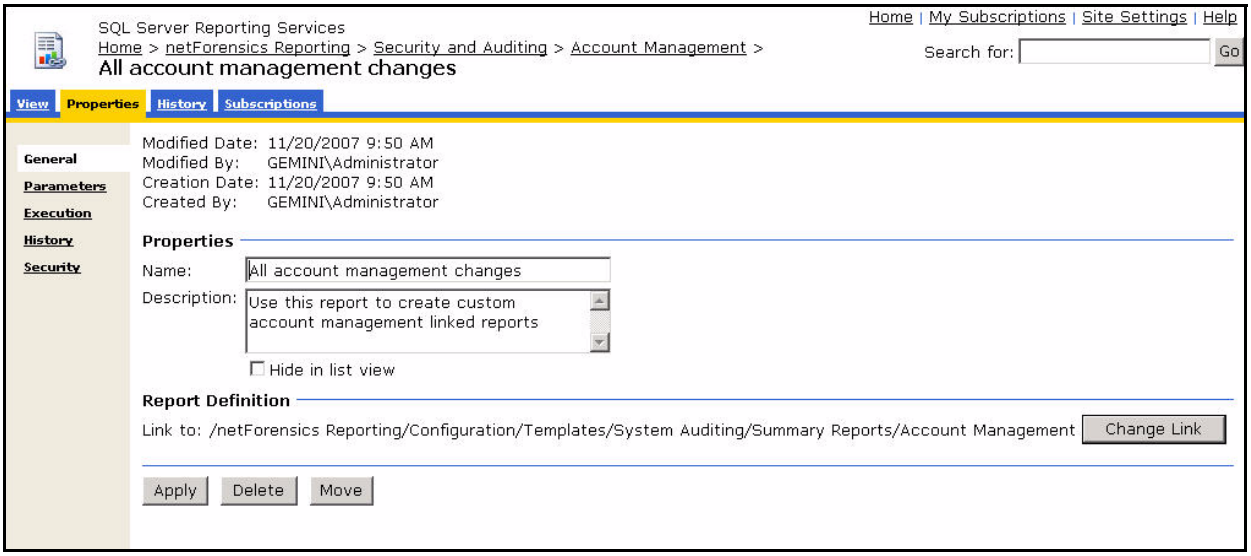


Figure 105: Report Manager screen: Report Properties

3. You can also rename the report here. Click the **Move** button.

   » The **Report Folder tree** structure screen appears.

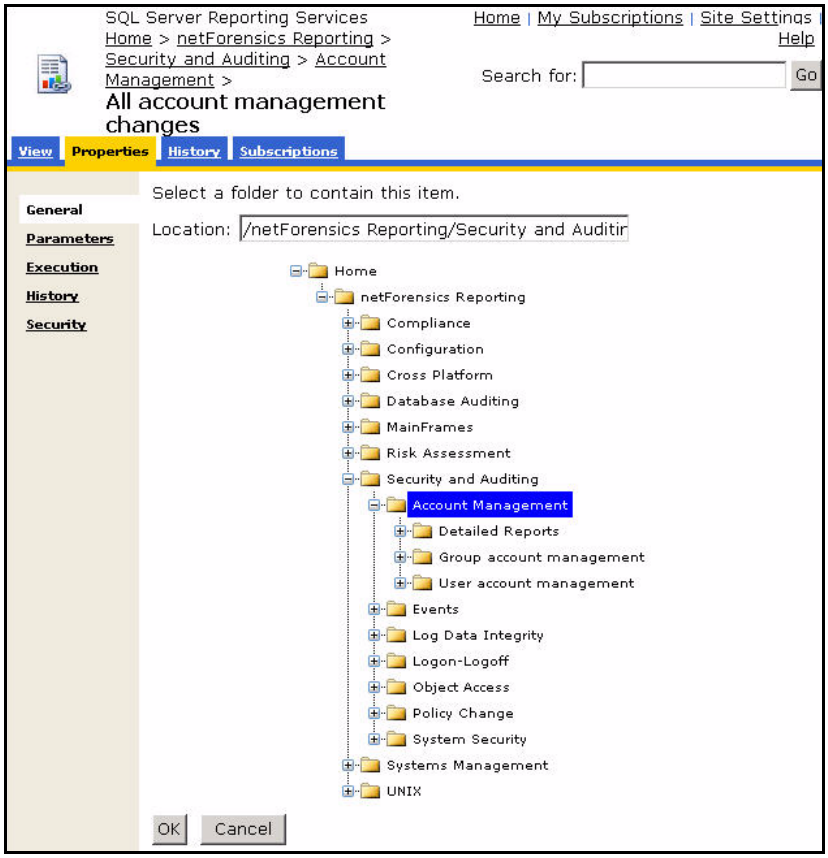


Figure 106: Report Folder tree

4. Highlight the folder where you want to move the report to.
5. Click the **OK** button.

» The Report has been moved to its new location.

Deleting Reports

There may be times when you want to **delete** a Report. The steps below will show you how to complete this task.

1. In **Report Manager**, open the folder that contains the Report that you would like to delete.
2. Open the **Report** you would like to delete.
3. Click the **Properties** tab.
4. Click the **Delete** button.
   » The Report has been deleted.

Changing Company Logos in a Report

netForensics Reporting allows you to change the company logo displayed on the Report's header. The steps below will show you how to complete this task:

1. Open **Report Manager** and browse to the ***netForensics Reporting > Configuration > Images*** folder.
   » The **Images** page appears.

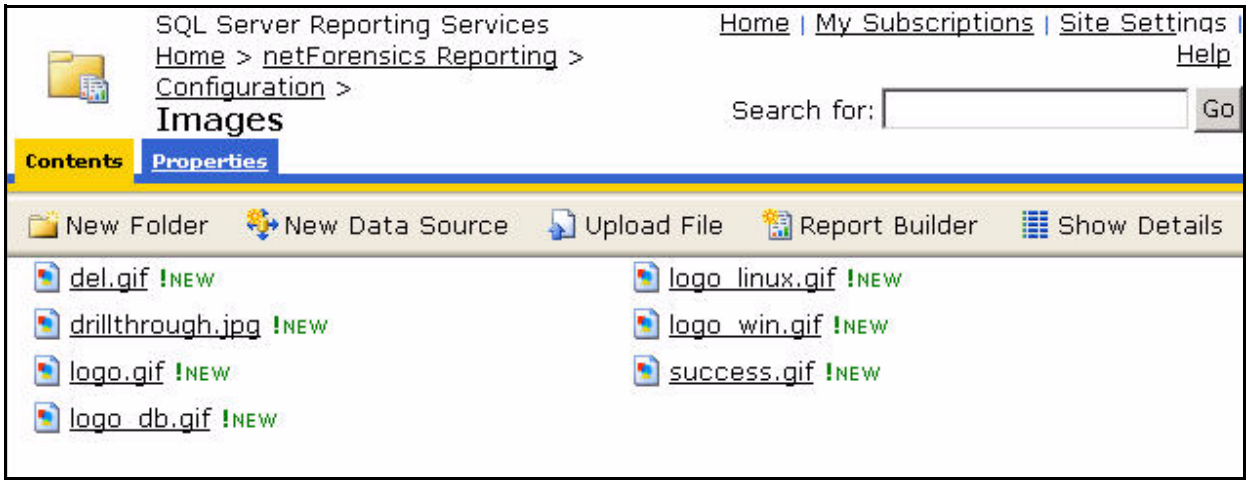


Figure 107: Report Manager screen: Changing a Company Logo

2. Select **Upload File** button from the icon bar.
   » The **Upload File** screen displays.



Figure 108: Report Manager : Upload File

3. Use the **Browse** button to locate the image that you want to upload.
4. Enter the name you would like to appear as the link on the page in the **Name** field.
5. Click the **OK** button.
6. Select **Refresh Image** from the Navigation tab to view the new logo for this Report.

Changing the Data Source DSN settings

There may be times when you will need to tell **netForensics Reporting** that either the database name or the SQL credentials used to access the database have changed. If this occurs, you must update **netForensics Reporting**. To change the data source DNS setting, follow these steps:

1. Open IE and browse to:
   `http://<nFX Log One_Reporting_Server_name>/RtReporting/console.aspx`

   Or from the Windows menu, select ***Start > All Programs > netForensics > Reporting > Web Console***

   » The **netForensics Web Console** screen appears.

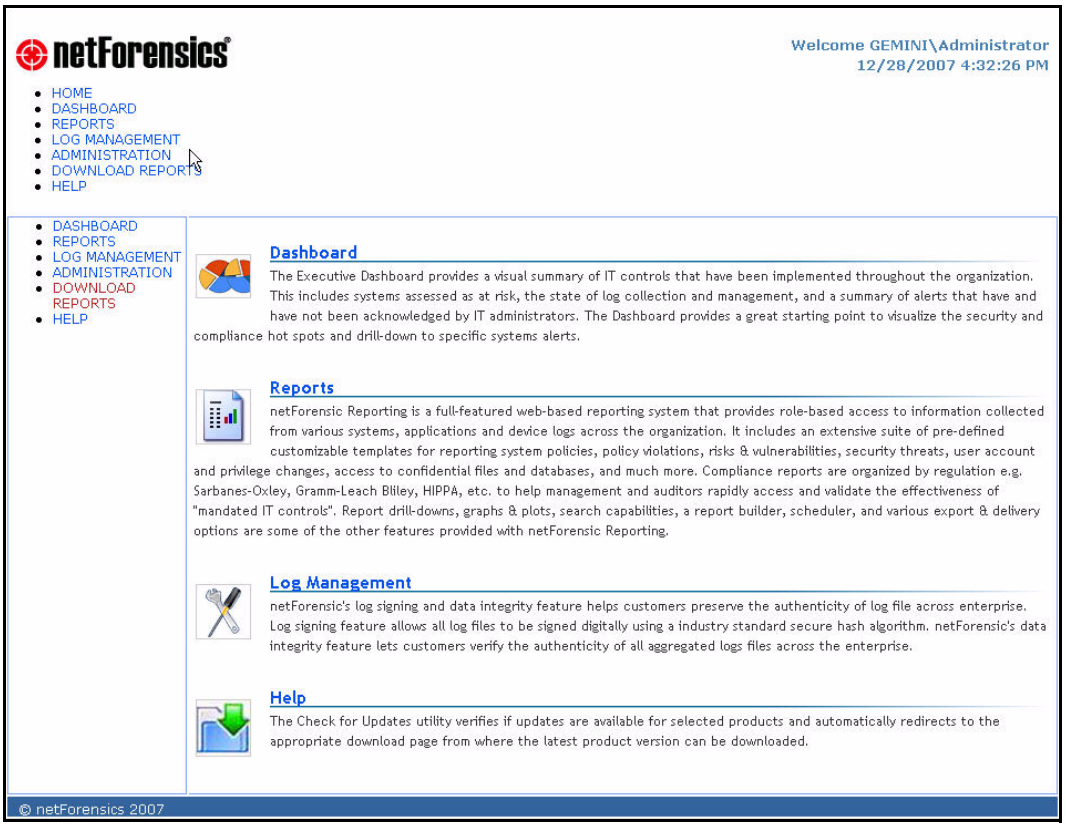


Figure 109: netForensics Web Console

2. Click on the **Administration** link in the left panel.

   » The **Report Administration** screen appears.

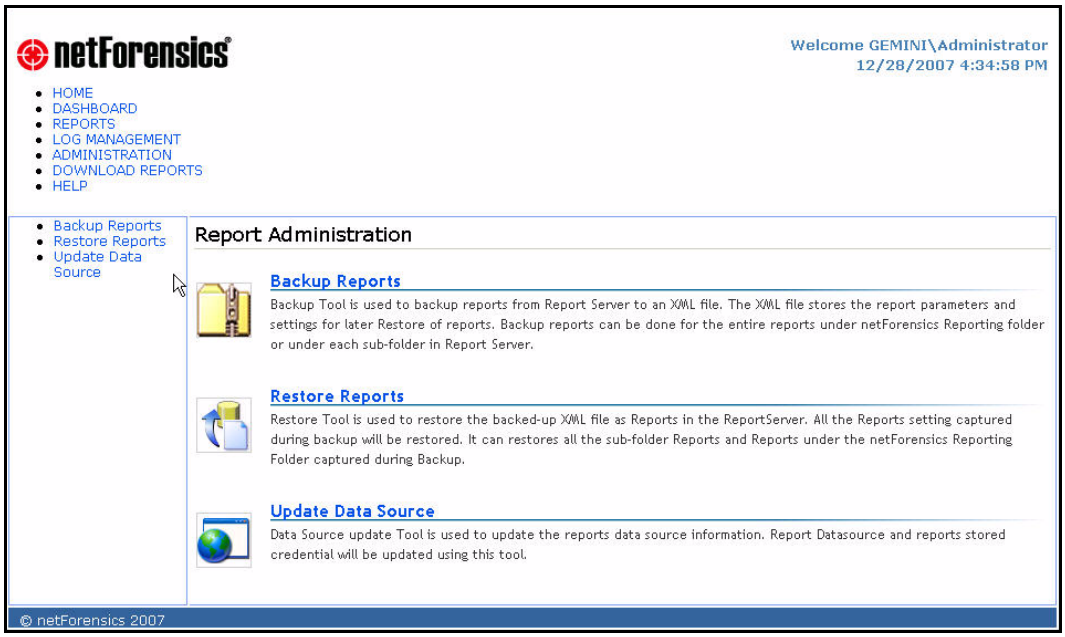


Figure 110: Web Console: Report Administration screen

3. Click the **Update Data Source** link.

» The **Update Data Source** screen is displayed.

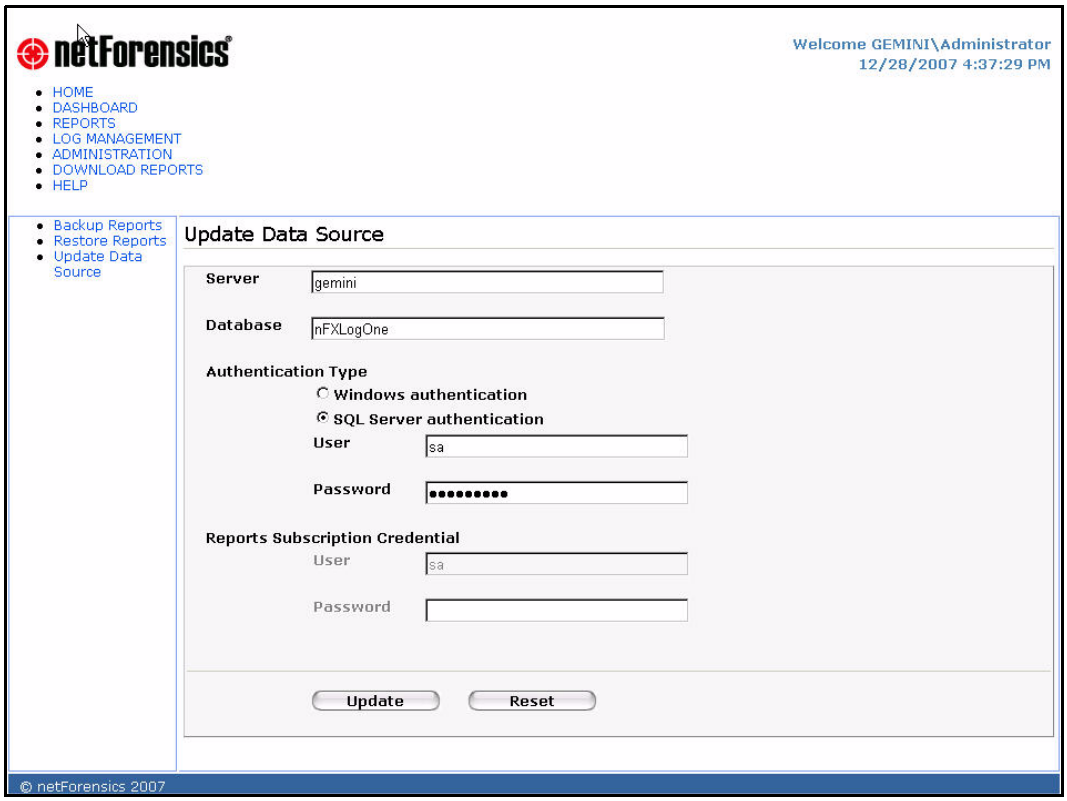


Figure 111: Web Console: Update Data Source screen

4. Enter the updated information and click **Update**.

Report History

Report History is a collection of previously run copies of a report. You can use **Report History** to maintain a record of a report over time. For more information please refer the following link: Report History.

Report Subscription

Report Subscriptions allow you to setup scheduled reports. **Reports Subscriptions** can be delivered in different formats to e-mail accounts or to file shares. **netForensics Reporting** allows you to create, edit, and delete Report Subscriptions. The steps below will show you how to complete these tasks.

1. Open a **Report** and click on the **New Subscription** icon located below the **Properties** tab.
   - » This example uses the **all account management changes** report.

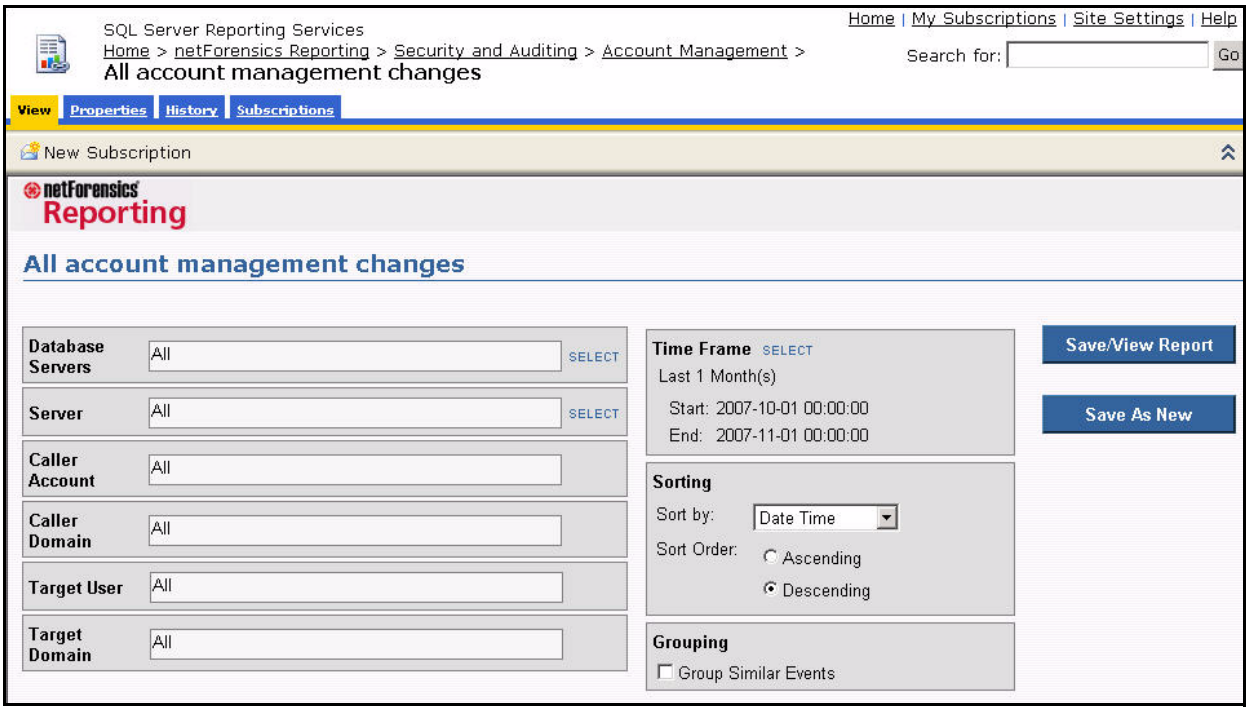


Figure 112: Report Delivery Options screen

Click the **New Subscription** link.

» The **Subscription** page appears.

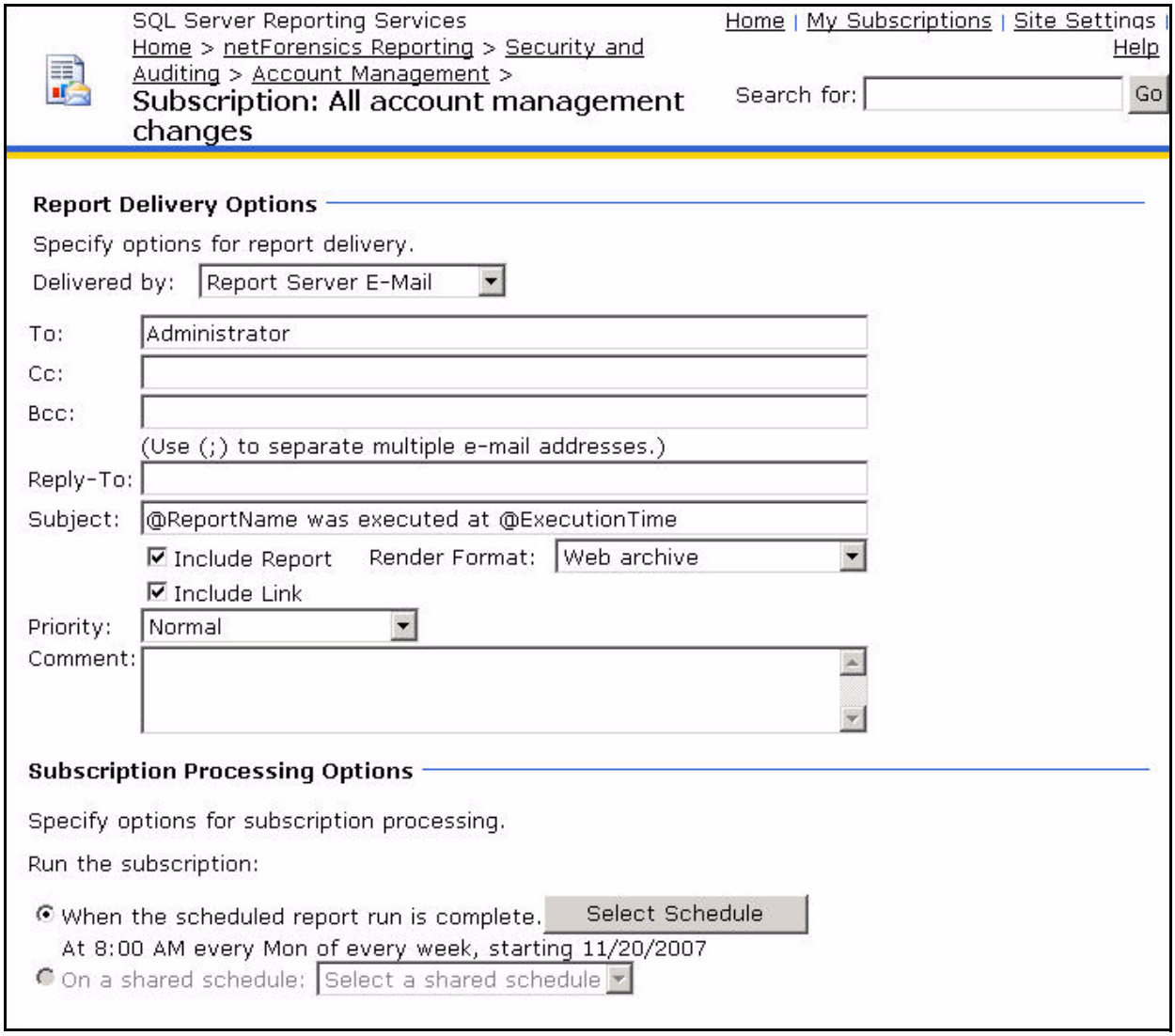


Figure 113: New Subscription page: Report Delivery Options

2. Enter the e-mail address(es) in the **To:**, **Cc:** and/or **Bcc:** fields.
3. Fill in the remainder of the form as needed.
4. Click on the **Select Schedule** button to select when the report should be delivered.

» The **Schedule Details** page appears.

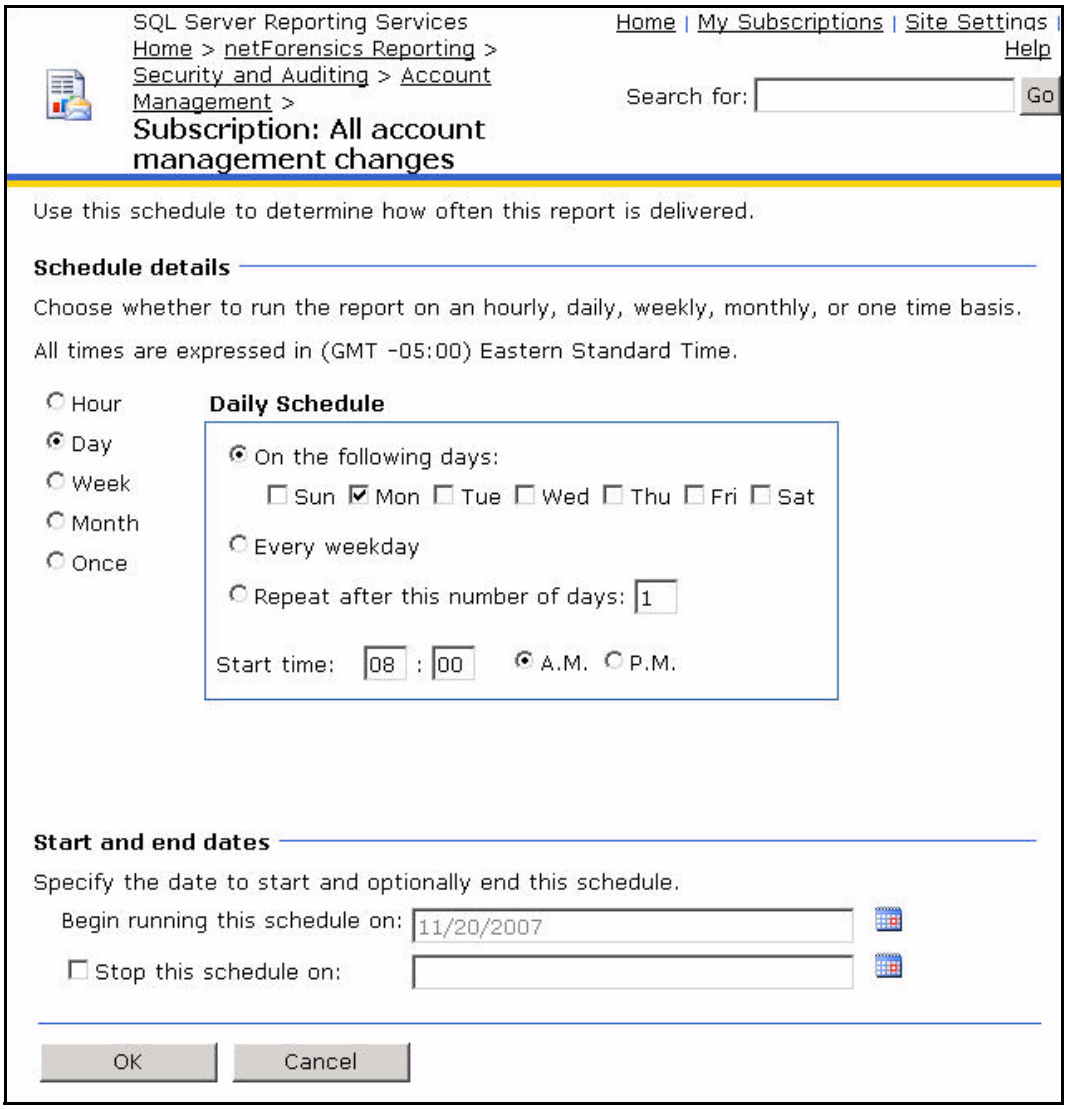


Figure 114: Report Schedule Details screen

5. Set the desired schedule.
6. Click the **OK** button to save.
   » The **New Subscription page: Report Delivery Options** screen displays.
7. Click the **OK** button to save the **Report Subscription**.

For more information please refer the following link: Report Subscriptions.

Report Access and Role Assignments

You can utilize **Report Access and Role Assignments** to create permissions for users and determine how they access and administer **Reporting Services**.

1. Open the **Report Manager** (SQL Reporting Services Home page).

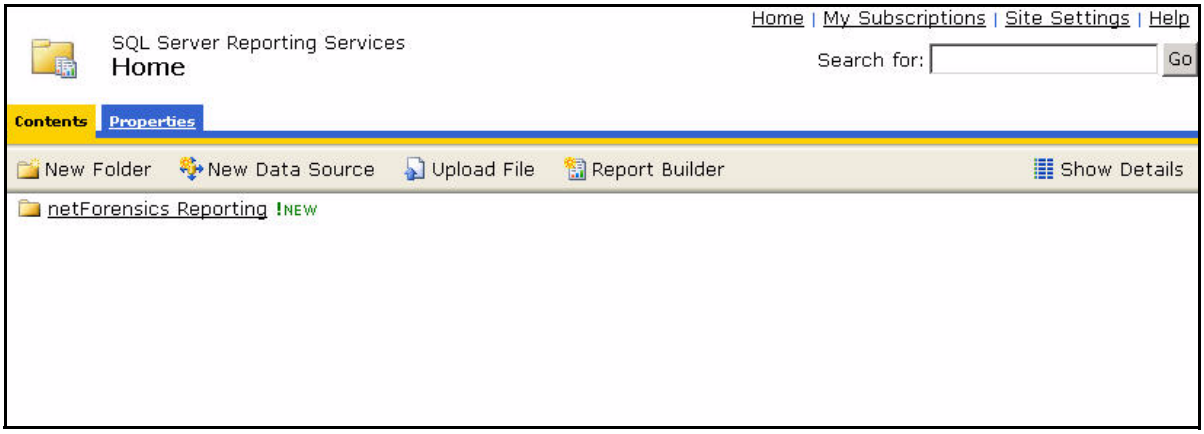


Figure 115: SQL Server Reporting Services Home page

2. Click the **Properties** tab.

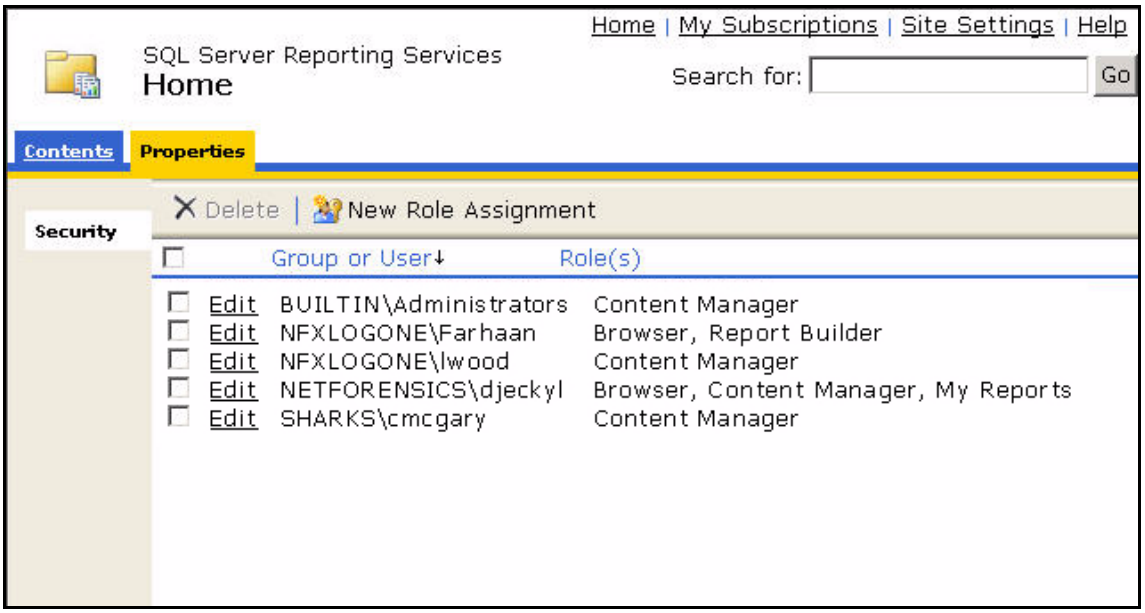


Figure 116: SQL Server Reporting Services screen: Properties tab

3. Click on **New Role Assignment** button on toolbar.

» The **New Role Assignment** screen displays.

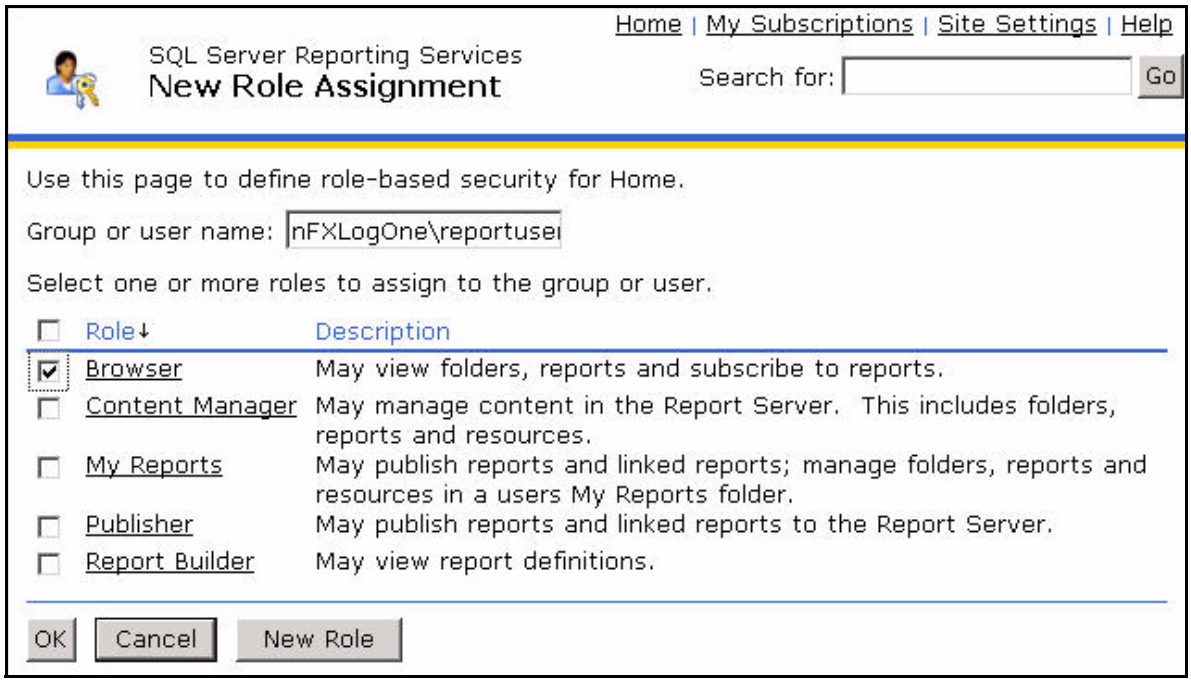


Figure 117: New Role Assignment screen

4. Here you can add an existing domain user, domain group account or a local report users group. This local group can contain domain accounts where administrative access is not allowed.
5. Select the **checkbox** next to the role you want to assign to a specific **User** or **Group**.
6. Click the **OK** button.

For more information please refer the following link: Report Access and Role Assignments.

Notes: