Installation and Configuration Guide

NetIQ® Security Manager
UNIX Agent

March 2014

Legal Notice

Contents

About this Book and the Library

This book provides conceptual and installation information about the agent that provide support for UNIX and Linux computers running the NetIQ Security Manager product. This book defines terminology and includes implementation scenarios.

Intended Audience

This book provides information for individuals responsible for understanding administration concepts and implementing a secure, distributed administration model.

Other Information in the Library

The Security Manager library provides the following information resources:

Installation Guide

Provides detailed planning and installation information about Security Manager.

User Guide

Provides conceptual information about Security Manager. This book also provides an overview of the user interfaces and step-by-step guidance for many administration tasks.

Help

Provides context-sensitive information and step-by-step guidance for common tasks, as well as definitions for each field on each window.

About NetIQ Corporation

We are a global, enterprise software company, with a focus on the three persistent challenges in your environment: Change, complexity and risk—and how we can help you control them.

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

Enabling critical business services, better and faster

We believe that providing as much control as possible to IT organizations is the only way to enable timelier and cost effective delivery of services. Persistent pressures like change and complexity will only continue to increase as organizations continue to change and the technologies needed to manage them become inherently more complex.

Our Philosophy

Selling intelligent solutions, not just software

In order to provide reliable control, we first make sure we understand the real-world scenarios in which IT organizations like yours operate—day in and day out. That's the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that's so much more rewarding than simply selling software.

Driving your success is our passion

We place your success at the heart of how we do business. From product inception to deployment, we understand that you need IT solutions that work well and integrate seamlessly with your existing investments; you need ongoing support and training post-deployment; and you need someone that is truly easy to work with—for a change. Ultimately, when you succeed, we all succeed.

Our Solutions

- Identity & Access Governance
- Access Management
- Security Management
- Systems & Application Management
- Workload Management
- Service Management

Contacting Sales Support

For questions about products, pricing, and capabilities, contact your local partner. If you cannot contact your partner, contact our Sales Support team.

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	1-888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, contact our Technical Support team.

Worldwide:	www.netiq.com/support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Web Site:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, click **Add Comment** at the bottom of any page in the HTML versions of the documentation posted at www.netiq.com/documentation. You can also email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

Qmunity, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, Qmunity helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, visit http://community.netiq.com.

1 Introduction

The NetIQ UNIX Agent enables UNIX and Linux operating system support for the following NetIQ products:

- NetIQ AppManager
- NetIQ Change Guardian
- NetIQ Secure Configuration Manager
- NetIQ Security Manager
- NetIQ Sentinel

The NetIQ UNIX Agent includes the following components:

- NetIQ UNIX Agent Manager: A user interface that you can use to manage all your UNIX agents components across your enterprise. UNIX Agent Manager runs on Windows, Solaris, and Linux operating systems. You can store information about your agent computers in one UNIX Agent Manager server, then access the information through one or numerous UNIX Agent Manager consoles.
- The AppManager UNIX Agent: A component of the NetIQ UNIX Agent that enables support for AppManager and provides the managed objects for UNIX and Linux AppManager modules.
- The NetIQ Security Agent for UNIX: A component of the NetIQ UNIX Agent that enables support for Change Guardian, Secure Configuration Manager, and Security Manager.
- Common components: Components that are shared by the AppManager UNIX Agent and the Security Agent for UNIX.

1.1 Overview of Features

Securing and monitoring the performance of your UNIX and Linux environment can be expensive and time-consuming, especially when you and your staff face tight budgets and escalating security threats. Consider the following issues most enterprise performance and security managers face:

- Deficits in staff knowledge concerning UNIX and Linux security and system expertise
- Managing various operating systems including Red Hat, AIX, HP-UX, Solaris, and SUSE Linux
- Controlling access to privileged commands and sensitive resources
- Lacking intrusion detection and response systems to handle both real and potential security breaches

The NetIQ Security Agent for UNIX (UNIX agent) helps you effectively address these challenges, enabling Security Manager to monitor the security of your UNIX and Linux environment.

1.2 What is the UNIX Agent?

The **NetIQ Security Manager UNIX Agent** (UNIX agent) validates the configuration of UNIX and Linux endpoints to ensure compliance with corporate security policies and pinpoint potential vulnerabilities. An endpoint represents an agent-monitored operating system, application, web server, or database instance. You can install and configure your UNIX agent manually, or you can use UNIX Agent Manager.

1.3 What is UNIX Agent Manager?

UNIX Agent Manager allows you to install and configure all your UNIX agent components across your enterprise instead of interacting with the agents individually. UNIX Agent Manager also allows you to see any UNIX computers that NetIQ Security Manager, NetIQ Sentinel, NetIQ AppManager, and NetIQ Change Guardian products monitor. UNIX Agent Manager includes a console and a server that stores information and communicates with the agents. You can install numerous consoles that can connect to a single server. UNIX Agent Manager runs on Windows, Solaris, and Linux computers.

1.4 What are the UNIX Agent Processes?

The two key processes used by the UNIX agent are:

- **VigilEntAgent**: The process that the UNIX agent uses.
- **detectd**: The process that performs the monitoring tasks and data retrieval for Security Manager. The specific behavior of this process is directed by the content of the `detect.xml` file.

2 Installing and Licensing

This chapter provides information about installing, licensing, upgrading, and uninstalling the UNIX agent on computers you want to monitor. This chapter also provides an overview of starting and stopping the UNIX agent.

This chapter assumes you have Security Manager installed. For more information about installing Security Manager or about Security Manager system requirements, see the *Installation Guide for Security Manager*, which is available on the Security Manager Documentation page.

To install UNIX agent, complete the following checklist:

❑	Ensure you have the necessary environment. For more information, see Section 2.1, "System Requirements," on page 11.
❑	Install or upgrade UNIX Agent Manager. If you are upgrading, ensure you export your existing information before upgrading. If you are upgrading from UNIX agent version 7.1, use UNIX Agent Manager 7.3 or earlier. See Section 2.2, "Installing or Upgrading UNIX Agent Manager," on page 13.
❑	Install or upgrade the agent version 7.2 on the computer you want to manage. ◆ For information about how to install, or deploy, to one or more computers from the console, see Section 2.3.1, "Deploying the UNIX Agent Using UNIX Agent Manager," on page 14. ◆ For information about how to install on a local computer, see Section 2.3.3, "Installing or Upgrading the Agent on the Local Computer," on page 15. ◆ For information about how to install using an answer file, see Section 2.3.4, "Silently Installing on the Agent Computer," on page 16.
❑	Install any agent hotfixes applicable to your environment. For information about how to install patches to the console and the UNIX agent, see Section 2.4, "Applying Patches," on page 17. For a list of available hotfixes, see the Security Manager Hotfix page.
❑	Begin monitoring your UNIX and Linux computers.

2.1 System Requirements

For the latest information about specific supported software versions and the availability of module updates, visit the Security Manager Supported Products page.

The UNIX agent, when used with Security Manager, has the following system requirements.

Item	Requirement
NetIQ Security Manager	6.5.4 with hotfix 7010344. For information about hotfix 7010344, see the Security Manager Hotfixes page.

Item	Requirement
Operating system on agent computers	One of the following: ◆ CentOS ◆ HP-UX ◆ IBM AIX ◆ Oracle Linux ◆ Oracle Solaris ◆ Red Hat Enterprise Linux ◆ SUSE Linux Enterprise Server
Operating system on UNIX Agent Manager computers	One of the following: ◆ Red Hat Enterprise Linux ◆ SUSE Linux Enterprise Server ◆ Windows 7 (32-bit and 64-bit) ◆ Windows 8 ◆ Windows Server 2008 R2 ◆ Windows Server 2008 (32-bit and 64-bit) ◆ Windows Server 2012
Memory on agent computers	512 MB
Memory on UNIX Agent Manager	UNIX agents require the following: ◆ 128 MB minimum RAM ◆ 512 MB swap file (virtual memory)
Hard disk space on agent computers	350 MB plus 400 Bytes per inode used by local file systems
Hard disk space on UNIX Agent Manager computers	1.2 GB
Default port assignments	UNIX agent uses the following default ports: ◆ 2620: The UNIX agent communicates with UNIX Agent Manager. ◆ 1622: The UNIX agent communicates with Security Manager. You can use the **Configure** option in UNIX Agent Manager to change the port assignments.

Item	Requirement
Accounts	The UNIX Deployment wizard uses the `su` command to access the root account on the computer on which you want to install UNIX agents. The root password is used by the wizard only at installation and is not stored. If you cannot use the root account, you can deploy using an account with sudo privileges. **NOTE:** (Conditional) If you are using an account with sudo privileges on a SUSE computer, be aware that the default SUSE configuration requires that the sudo account log in using the root password instead of the account's password.

2.2 Installing or Upgrading UNIX Agent Manager

NetIQ UNIX Agent Manager is a console that you can use to manage all your UNIX agent components across your enterprise. UNIX Agent Manager runs on Windows and Linux. You can use UNIX Agent Manager to install to several computers at the same time. UNIX Agent Manager also allows you to see any UNIX computers that other NetIQ products monitor.

UNIX Agent Manager version 7.2 added a server component and a console. If you use UNIX agent version 7.2 or higher, you must use UNIX Agent Manager version 7.2 or higher. However, you can use UNIX Agent Manager version 7.2 or higher with older versions of the UNIX agent. The following procedure guides you through installing or upgrading UNIX Agent Manager components.

2.2.1 Installing UNIX Agent Manager on a Microsoft Windows Computer

Complete the following steps to install the either the UNIX Agent Manager server, the UNIX Agent Manager console, or both on a Windows computer.

To install UNIX Agent Manager on a Windows computer:

1. Log on to the Windows computer using a local administrator account.
2. (Conditional) If you are upgrading, save the information for your existing agents to a file using the **Export/Import Host Lists** menu option in UNIX Agent Manager. When the export completes, remove the program using the Remove Programs utility in the Windows operating system or the Uninstall UNIX Agent Manager utility from the NetIQ program group.
3. Run `UAMInstaller.MSI` in the root folder of the installation kit, and begin responding to the questions in the wizard.
4. When you are given the option of communication security settings, do not restrict communication to only Federal Information Processing Standard (FIPS) encrypted algorithms. If you select that option, you cannot use UNIX Agent Manager with Security Manager.
5. Complete the automatic installer wizard. The wizard guides you through the Trial Software License Agreement and installs the UNIX Agent Manager to the folder that you specify.
6. Type and confirm a password that the UNIX Agent Manager server will use for the admin user account.
7. (Conditional) If you are upgrading from UNIX Agent Manager version 7,1, import your agent information using the **Import 7.1 Host List** under the **File** menu.

2.2.2 Installing UNIX Agent Manager on a Linux Computer

Complete the following steps to install the either the UNIX Agent Manager server, the UNIX Agent Manager console, or both on a Linux computer.

To install the UNIX Agent Manager on a Linux computer:

1. Change directories to where you copied the installation package for UNIX Agent Manager. In the installation package, change directories to where the installation files are located.
2. Extract the appropriate `.tar.gz` file for your platform.
3. In the new `UAM` folder, start the installation by running `./installserver.sh install`.
4. Type and confirm a password that the UNIX Agent Manager server will use for the admin user account.
5. Start the UNIX Agent Manager console by running the `run.sh` script.

2.3 Installing and Upgrading the Agent

You can install the agent locally on the computer you will monitor, by deploying from UNIX Agent Manager, or without user interaction by using an answer file.

2.3.1 Deploying the UNIX Agent Using UNIX Agent Manager

Remote deployment provides a convenient and uniform method for installing one or more UNIX agents. You can use the Deployment wizard provided in the UNIX Agent Manager for remote deployment, unless one of the following conditions exists:

- Your site standards prohibit your access to root passwords.
- Your site standards require a specific software distribution mechanism.
- Your site standards prohibit software distribution mechanisms.

For information about installing UNIX Agent Manager, see Section 2.2, “Installing or Upgrading UNIX Agent Manager,” on page 13.

To remotely deploy UNIX agent components:

1. In the **File** menu of UNIX Agent Manager, select **Remote Deployment**.
2. Click the **Add Host** button and fill in the fields as prompted.
3. When you are given the option of communication security settings, do not restrict communication to only Federal Information Processing Standard (FIPS) encrypted algorithms. If you select that option, you cannot use UNIX Agent Manager with Security Manager.
4. When you are given the option to specify the restart method, NetIQ recommends that you accept the default, rclink. For more information about restart methods, see Section 3.6, “Restart Methods for the UNIX Agent,” on page 26.
5. Proceed through the wizard to complete installation.
6. When the installation completes, register the agent in Security Manager.

2.3.2 Upgrading UNIX Agent version 7.1 Using UNIX Agent Manager

UNIX Agent Manager provides a utility to upgrade existing agents.

To upgrade version 7.1 UNIX agents using UNIX Agent Manager version 7.2 or higher:

1. Ensure the computer that you want to upgrade is registered in UNIX Agent Manager. You can do this by either importing an existing list that contains the computer using **Manage Hosts** > **Import/Export Host Lists**, or by adding the computer using **Manage Hosts** > **Add Host**.
2. Highlight the computer you want to upgrade, and select **Manage 7.1 Hosts** > **Upgrade Hosts**. The left pane will display any options you need to select for your agent.
3. Scroll to the bottom of the panel and click the **Start Upgrade** button.
4. When the upgrade completes, register the agents in Security Manager by removing the agents and adding them back. If you were sending real-time events to Security Manager, also change the port to 1637.

2.3.3 Installing or Upgrading the Agent on the Local Computer

The following procedure guides you through logging on to an agent computer and locally installing all required components on the agent computer. If you are upgrading and have used UNIX Agent Manager, make sure to export your host list.

To install or upgrade an agent on the local computer:

1. (Conditional) If you are upgrading and use UNIX Agent Manager, ensure you have upgraded UNIX Agent Manager. For information about upgrading UNIX Agent Manager, see Section 2.2, "Installing or Upgrading UNIX Agent Manager," on page 13.
2. Log on to an agent computer using an account with super user privileges.
3. Change directories to the product installation package, and then enter the following command to start the install script:

   ```
   /bin/sh ./install.sh
   ```

4. Proceed through the prompts.
5. When you are given the option to configure the agent for use with other products, select the option only if you run NetIQ AppManager, NetIQ Change Guardian, or NetIQ Secure Configuration Manager to monitor the computer. If you will not use those products, type n instead of accepting the default response of y for those questions.
6. When you are given the option to specify the restart method, NetIQ recommends that you accept the default, rclink. For more information about restart methods, see Section 3.6, "Restart Methods for the UNIX Agent," on page 26.
7. (Conditional) If you are installing for the first time, register the agent in Security Manager.
8. (Conditional) If you are upgrading, register the agents in Security Manager by removing the agents and adding them back. If you were sending real-time events to Security Manager, also change the port to 1637.

When you finish the installation process, the UNIX agent starts the daemons.

2.3.4 Silently Installing on the Agent Computer

Performing a silent installation allows you to install the UNIX agent without interactively running the installation script. Instead, silent installation uses an installation file that records the information required for completing the installation. Each line in the file is a *name=value* pair that provides the required information, for example, `HOME=/usr/netiq`.

If you use the deployment wizard to perform a local installation on one computer, the wizard offers you an opportunity to create a silent installation file based on your choices. A sample installation file, `SampleSilentInstallation.cfg`, is located on your UNIX agent download package. The following parameters are available for silent installation for the NetIQ UNIX Agent 7.2 or higher working with Security Manager:

Parameter	Description
`FRESH_INSTALL`	Specifies whether you want to install or upgrade the agent. If you upgrade, some entries in the silent install file are not required. Valid entries are `1` (install) and `0` (upgrade). When FRESH_INSTALL is set to `1`, the install script overwrites any installed agent with a new copy of the agent. When FRESH_INSTALL is set to `0`, the install script adds components to an existing install. The default is `1`.
`CREATE_TARGET_DIR`	Specifies whether you want the install program to create the target installation directory if it does not already exist. Valid entries are `y` and `n`. The default is `y`.
`CONTINUE_WITHOUT_PATCHES`	Specifies whether the install program stops or continues when the operating system is not a supported version. Valid entries are `y` and `n`. The default is `n`.
`IQCONNECT_PORT`	Specifies the port that the UNIX agent uses to listen for communications from UNIX Agent Manager. The default is `2620`.
`IQ_STARTUP`	Specifies restart method for the uagent process. For information about the options, see Section 3.6, “Restart Methods for the UNIX Agent,” on page 26. Valid entries are `rclink` and `inittab`. The default is `rclink`.
`USE_FIPS_COMMON`	Specifies whether the UNIX agent communicates with UNIX Agent Manager using only FIPS certified encryption algorithms. Do not use this option when using the agent with Security Manager. The default is `0`.
`INSTALL_SM`	Specifies whether the UNIX agent works with Security Manager. Valid entries are `y` and `n`.
`SM_CENTRAL_ADDR`	Specifies the IP address of the Security Manager Central Computer.
`SM_CENTRAL_PORT`	Specifies the port that the UNIX agent will use to communicate with the Security Manager Central Computer.
`SM_SNMP_TRAPS`	Specifies the port that the UNIX agent will monitor for SNMP notifications.

Parameter	Description
SM_LOW_DISK	Specifies the minimum disk space in bytes that are required to run the UNIX agent for Security Manager. If the disk space falls below this limit, then the agent will stop monitoring.
SM_Domain	(Optional) If you want a specify a custom name for the UNIX agent, specify it here.
SM_STARTUP	Specifies restart method for the UNIX Agent. For information about the options, see Section 3.6, "Restart Methods for the UNIX Agent," on page 26. Valid entries are `rclink` and `inittab`. The default is `rclink`.

Once you have created the installation file, you can run the silent installation from the command line. For example:

```
./install.sh <Target_Directory> -s <SilentConfigurationFile>.cfg
```

Where <Target_Directory> is the directory you want to install to and <SilentConfigurationFile> is the file name you used to specify the installation options. You can also use the default configuration file, `SampleSilentInstallation.cfg`. The installation filename must be specified as an absolute path. By default, SampleSilentInstallation.cfg is located in the UNIX agent install directory.

The script extracts information from the installation file and installs the agent according to the values you specify.

Once you have completed the silent installation of the agent, register the agent in Security Manager. If you are upgrading, register the agents in Security Manager by removing the agents and adding them back. If you were sending real-time events to Security Manager, also change the port to 1637.

2.4 Applying Patches

NetIQ provides patches to the UNIX agent in a zipped file known as a **p-ball**.

Patches to UNIX Agent Manager are applied to the UNIX Agent Manager server, which automatically applies any required changes to the consoles using that server. To update UNIX Agent Manager on Windows, click **Update UAM** on the Start menu. To update UNIX Agent Manager on Linux, run the `update.sh` command.

To upgrade the agent computer using the UNIX Agent Manager:

1. Click **Patch > Patch Manager**.
2. Click **Load Patch** to add the patch you want to apply to the list of available patches.
3. Select the computers where you want to apply the patch.
4. Select the patch or patches that you want to apply.
5. Click **Start Install**. The time necessary to update your agents depends on the number of agents to update, distance from the UNIX Agent Manager server, network connectivity, and bandwidth, among other factors. This process can take up to 20 minutes per agent.
6. Click **Back** to close the Patch Manager.

2.5 Uninstalling UNIX Agents and UNIX Agent Manager

You can uninstall the UNIX agent components manually or using UNIX Agent Manager. If the agent you are uninstalling is registered in Security Manager for log collection, remove the agent from Security Manager before uninstalling.

2.5.1 Uninstalling the UNIX Agent

You can use UNIX Agent Manager to uninstall agents from remote computers, or you can uninstall them locally. When you uninstall the agent, you can choose to uninstall all components, or only one the are for specific products.

NOTE: You do not need to uninstall agents with a lower version number before upgrading agents. Use this procedure only if you want to completely remove agents from remote computers.

To uninstall the agent locally, change to the installation directory, then run the following command:

```
./uninstall.sh
```

You can also uninstall using the console. This option allows you to uninstall from many computers at once. To uninstall an agent in UNIX Agent Manager, select the computers where you want to uninstall the agent, click **Manage Hosts > Uninstall Agent**.

2.5.2 Uninstalling UNIX Agent Manager

To uninstall the UNIX Agent Manager on Windows computers, use the **Add/Remove Programs** Control Panel to remove the **UNIX Agent Manager** program.

To uninstall the UNIX Agent Manager on a Linux computer, change directories to the UNIX Agent Manager installation directory and run `installserver.sh` -remove. When you have completed the uninstall program, you can remove the UAM directory by running `rm -rf UAM`.

2.6 Licensing

The UNIX agent requires the use of a license key file. The Security Manager console requires a valid license. Ensure your licenses provide the appropriate coverage for your needs.

Your trial license allows you to experience the convenience and security of deployed NetIQ Security agents for up to one month. When you decide to move your trial into production, contact your NetIQ sales representative for a production license.

3 Working with the UNIX Agent and UNIX Agent Manager

This chapter describes features of the UNIX agent and UNIX Agent Manager beyond installation. This chapter also presents internal product concepts, such as communication between the components and restart options.

UNIX Agent Manager provides some features that this guide does not describe. The console provides these features for products other than Security Manager.

3.1 Configuring Basic Security Manager Support

Complete the following steps to activate the rule set delivered with the latest version of UNIX Agent Manager on your agent computers. These rules configure the event detection and alerting daemon to send events to Security Manager for real-time monitoring and spool events for Security Manager log management.

To deploy rule sets to agent computers:

1. Start the UNIX Agent Manager.
2. Click **Rules Manager**.
3. Make any changes you want to make to the default rule set displayed in the Rule Manager, customize the rule set as needed until the rule set is correctly configured for your environment. For more information about configuring custom rule set elements, see Chapter 4, "Understanding Security Rules," on page 29

   NOTE: You cannot use custom rule sets that you created for previous versions of the product with the current version of the product. However, you can manually copy and paste elements from your custom rule set to the default rule set. For more information about copying and pasting rule elements, see the Security Manager Help.
4. After you made changes to the rule set, save a copy by clicking **File > Save/Save All** and completing the Save window.
5. In the Available Hosts list, select the agent computers where you want to deploy the rule set.
6. Click **File > To Select Hosts**.
7. Click **Select** to deploy the rule set. The detectd process, which is a watchdog process, begins processing and initializing the new rule set immediately. However, it may take up to 30 seconds for the new rule set to take effect.
8. Click **Hosts > Scan All Hosts**.
9. Verify that the rule set is active on the agent computers. The **Security Manager** column shows green cells for all agents with an active rule set.

3.2 Configuring Extended Security Manager Support

The tasks in this section help you enable and configure process accounting on UNIX computers and the Basic Security Module on Solaris computers. Enabling this functionality provides additional auditing of security-related events beyond the scope of events that are logged to syslog.

Many security-related events are logged to the syslog facility, which is enabled by default on all UNIX operating systems supported by Security Manager. All events logged to syslog are sent to Security Manager. However, Security Manager can also process security-related events logged by modules that are not enabled by default, such as process accounting and the Basic Security Module on Solaris.

You can enhance security event reporting in Security Manager by enabling process accounting. You can also enable and configure the Basic Security Module on Solaris to map the events for real-time monitoring. However, enabling process accounting and the Basic Security Module substantially increases the activity on the monitored computer and also changes the base computer configuration, which may not be allowed per your site standards. Enabling process accounting and the Basic Security Module are optional tasks. Do not enable these modules if syslog reports the events you want to monitor.

3.2.1 Enabling Process Accounting

Enabling process accounting provides additional events to Security Manager. This section provides information about enabling process accounting and configuring rc scripts to automatically restart process accounting after a reboot.

Enabling Process Accounting on AIX Computers

The steps in this section help you start and restart process accounting on AIX computers.

To enable process accounting, enter the following command at the prompt:

```
/usr/sbin/acct/accton /var/adm/pact
```

You can also enter the following line in an rc script to automatically restart process accounting:

```
/usr/bin/su – adm –c /usr/sbin/acct/startup
```

Enabling Process Accounting on HP-UX Computers

The steps in this section help you start and restart process accounting on HP-UX computers.

To enable process accounting, enter the following command at the prompt:

```
/usr/sbin/acct/startup
```

You can also enter the following line in the `/etc/rc.config.d/acct` script to automatically restart process accounting:

```
START_ACCT=1
```

Enabling Process Accounting on Red Hat Linux

The steps in this section help you configure process accounting on Red Hat Linux computers.

To configure process accounting on Red Hat Linux computers:

1. Install the `psacct` package located in the Linux installation kit. This package is not installed by default unless you installed all available packages. For more information about installing the `psacct` package, see the Red Hat Linux documentation.
2. Modify your system init script to automatically start process accounting by adding the following lines:

   ```
   # Turn process accounting on.
   if [ -x /sbin/accton ]
   then
        /sbin/accton /var/log/pacct
        echo "Process accounting turned on."
   fi
   ```

3. Create an accounting record file named pacct by entering the following command:

   ```
   touch /var/log/pacct
   ```

   By default, the process accounting software prints out all commands executed to the file `/var/log/pacct`.

4. Modify the permissions to the `pacct` file by entering the following commands:

   ```
   chown root /var/log/pacct
   chmod 644 /var/log/pacct
   ```

Enabling Process Accounting on Solaris Computers

The steps in this section help you start and restart process accounting on Solaris computers.

To start process accounting, enter the following command at the prompt:

```
/usr/lib/acct/accton /var/adm/pacct
```

You can also enter the following commands to automatically restart process accounting:

```
ln /etc/init.d/acct /etc/rc2.d/S22acct
ln /etc/init.d/acct /etc/rc0.d/K22acct
```

3.2.2 Enabling and Configuring the Basic Security Module on Solaris

Security Manager can process events from the Basic Security Module on Solaris computers. Real-time monitoring can alert you to security events reported by the Basic Security Module. The steps in this section help you enable and configure the Basic Security Module. The steps also help you archive and delete audit log files.

Enabling the Basic Security Module

The Basic Security Module is disabled by default on Solaris computers. Complete the following steps to enable the Basic Security Module.

To enable the Basic Security Module:

1. Change directories to `/etc/security`.
2. Enter `./bsmconv` at the prompt to run a script that enables and configures the Basic Security Module to automatically restart after a reboot.

Configuring the Basic Security Module

You must configure the Basic Security Module to correctly map events for real-time monitoring. The steps differ slightly depending on which version you are using and your specific environment. For example, in Solaris 11, you can use the auditconfig command instead of directly editing the /etc/security/audit_control file. The following steps are guidelines based on Solaris 9.

To configure the Basic Security Module for real-time monitoring:

1. Modify the `/etc/security/audit_class` file by adding the following three lines:

   ```
   0x00010000:nb:NetIQ success&failure
   0x00020000:ns:NetIQ success
   0x00040000:nf:NetIQ failure
   ```

   between the following lines:

   ```
   0x00004000:ap:application
   0x20000000:io:ioctl
   ```

2. Modify the `/etc/security/audit_control` file by changing the flags as follows:

   ```
   flags:nb,+ns,-nf
   ```

3. Modify the `/etc/security/audit_event` file by appending `nb` or `nf` to the end of the lines as follows:

   ```
   2:AUE_FORK:fork(2):pc,nb
   4:AUE_CREAT:creat(2):fc,nb
   5:AUE_LINK:link(2):fc,nb
   6:AUE_UNLINK:unlink(2):fd,nb
   7:AUE_EXEC:exec(2):pc,ex,nb
   10:AUE_CHMOD:chmod(2):fm,nb
   11:AUE_CHOWN:chown(2):fm,nb
   23:AUE_EXECVE:execve(2):pc,ex,nb
   25:AUE_VFORK:vfork(2):pc,nb
   30:AUE_FCNTL:fcntl(2):fm,nb
   37:AUE_SETTIMEOFDAY:settimeofday(2):ad,nb
   38:AUE_FCHOWN:fchown(2):fm,nb
   39:AUE_FCHMOD:fchmod(2):fm,nb
   40:AUE_SETREUID:setreuid(2):pc,nb
   41:AUE_SETREGID:setregid(2):pc,nb
   42:AUE_RENAME:rename(2):fc,fd,nb
   43:AUE_TRUNCATE:truncate(2):fd,nb
   44:AUE_FTRUNCATE:ftruncate(2):fd,nb
   50:AUE_ADJTIME:adjtime(2):ad,nb
   72:AUE_OPEN_R:open(2) - read:fr,nf
   73:AUE_OPEN_RC:open(2) - read,creat:fc,fr,nf
   74:AUE_OPEN_RT:open(2) - read,trunc:fd,fr,nb
   ```

```
75:AUE_OPEN_RTC:open(2) - read,creat,trunc:fc,fd,fr,nb
76:AUE_OPEN_W:open(2) - write:fw,nb
77:AUE_OPEN_WC:open(2) - write,creat:fc,fw,nb
78:AUE_OPEN_WT:open(2) - write,trunc:fd,fw,nb
79:AUE_OPEN_WTC:open(2) - write,creat,trunc:fc,fd,fw,nb
80:AUE_OPEN_RW:open(2) - read,write:fr,fw,nb
81:AUE_OPEN_RWC:open(2) - read,write,creat:fc,fw,fr,nb
82:AUE_OPEN_RWT:open(2) - read,write,trunc:fd,fr,fw,nb
83:AUE_OPEN_RWTC:open(2) - read,write,creat,trunc:fc,fd,fw,fr,nb
111:AUE_CORE:process dumped core:fc,nb
201:AUE_STIME:old stime(2):ad,nb
214:AUE_SETEGID:setegid(2):pc,nb
215:AUE_SETEUID:seteuid(2):pc,nb
241:AUE_FORK1:fork1(2):pc,nb
```

4 Change the init level or reboot the computer to restart the Basic Security Module.

Manually Archiving and Deleting Audit Logs

The Basic Security Module creates audit log files that can grow to a considerable size. You can manually archive and delete audit log files.

To manually archive and delete audit logs:

1 Change directories to the audit log directory, `/var/audit/` by default.

NOTE: You can define the directory where logs are stored by modifying the `/etc/security/audit_control` file.

2 Copy the audit logs to your archive directory.

3 Delete the original audit logs, except for the log file with `not_terminated` in the filename. This is the active audit log and is typically the last file in the list.

3.2.3 Restricting Access to Rule Sets

The UNIX agent provides commands that allow you to customize the access to rule sets. Some environments might benefit from limiting access to the rule sets to improve security or performance. The following table describe the commands.

Command	Description
`DETECTD_OPS`	This commands allows you to define opcodes or opgroups allowed to access the rule sets. Separated the opcodes or opcode groups with a space. If you want to include an opcode group, but deny access to one of the opcodes in that group, prepend the opcode with a hyphen (-). Example: `DETECTD_OPS="sleep time unpack sort :browse"`
`DETECTD_SAFE_MODULES`	This command allows you to define which Perl modules _loadModule() loads. Separate the modules with a space. You can use wildcards to replace a single character or a set of characters. Example: `DETECTD_SAFE_MODULES="NONE"`

Command	Description
DETECTD_TOUCH_ALLOW	This command allows you to define which log files _touchLogfile() creates. Separate the file names with a space. You can use wildcards to replace a single character or a set of characters. Example: `DETECTD_TOUCH_ALLOW="/var/adm/pacct /var/account/pacct"`
DETECTD_TRUNC_ALLOW	This command allows you to define which log files _truncateLogfile() creates. Separate the file names with a space. You can use wildcards to replace a single character or a set of characters. Example: `DETECTD_TRUNC_ALLOW="/audit/stream.out"`
DETECTD_CMD_PATH	This command allows you to define the directories for command actions. Separate the file names with either a comma or a space. Example: `DETECTD_CMD_PATH="../local/script"`
DETECTD_LOG_DIR	This command allows you to define the directory for log actions. Example: `DETECTD_LOG_DIR="../local/log"`

3.3 Configuring Security Manager Support for Oracle

As a part of the steps to configure Security Manager to monitor Oracle, register the Oracle database and specify an account that has access to read the table and views. You can perform these steps on the UNIX Agent Manager computer.

NOTE: You only need to register the Oracle database and endpoint if you are not also running Secure Configuration Manager on your UNIX Agent Manager computer.

You must also ensure you have installed and configured the appropriate Security Manager modules. For more information about the overall process of configuring Security Manager to monitor Oracle, see *Security Manager for Oracle on UNIX*, which is available in the following folder on the Security Manager user interface computer:

```
installation folder\Program Files\NetIQ Security
Manager\OnePoint\Documentation\Module Documentation
```

Where *installation folder* is the location where you installed Security Manager user interfaces.

To register the Oracle database and specify an account with permission to read the table and views:

1. Start UNIX Agent Manager using an account that has permission to read the Oracle database (tables and views) that you want to monitor.
2. On the Hosts menu, click **Configure Agent > Configure Security Agent**.
3. Select the host with the Oracle database you want to monitor.
4. Click **Register Oracle Endpoint**.

5 Complete the fields on the window.

6 Click **OK**.

7 Activate the Oracle rule set. For more information about activating rule sets, see Section 3.1, "Configuring Basic Security Manager Support," on page 19.

3.4 Configuring Failover or Multiple Configuration Groups

If you do real-time monitoring, you can configure the UNIX agent to send data to multiple configuration groups. You can also specify redundant central computers in the event that the primary central computer becomes unavailable. You configure failover or multiple configuration groups with UNIX Agent Manager.

3.5 Managing Users in UNIX Agent Manager

UNIX Agent Manager allows administrators to control user access to features and computers. To log into any UNIX Agent Manager server, an administrator on that server must create the user account in the UNIX Agent Manager Administrator Console, which is part of the UNIX Agent Manager console.

You can grant different permissions to each user account that allows access to only the features required by that user's role. Permission sets allow you to simplify this process. Permission sets define product, computer, and feature access. Once you create a permission set, you can assign it to multiple user accounts with the same role.

For example, you can create a permission set that grants access to all Security Manager functionality separate from Secure Configuration Manager functionality. You can then assign this permission set to all computers running Security Manager. When you grant a new Security Manager user access to a console, simply assign the user to the Security Manager permission set to grant them access to the applicable features and computers.

To assign permissions, log into a UNIX Agent Manager console as an administrator and click **Access Control** > **Admin Console**. From there, add the users that need access to that UNIX Agent Manager server, then assign the appropriate permissions.

3.5.1 Using LDAP or Microsoft Active Directory Credentials

UNIX Agent Manager can access the information you have already set up in your LDAP or Microsoft Active Directory server to allow users to log into the UNIX Agent Manager server. This functionality is not available if you restricted UNIX Agent Manager to only use Federal Information Processing Standard (FIPS) encrypted algorithms.

To configure UNIX Agent Manager server to use LDAP or Active Directory credentials:

1. Ensure you have the following information:
   - The domain and computer address, such as ldap://houston.itservice.production:389, of the LDAP or Active Directory server
   - The location of the user entries in the structure of the LDAP or Active Directory server
   - The attribute that identifies the login name for each user
   - An account that UNIX Agent Manager server can use to access the LDAP or Active Directory server
2. Log into a UNIX Agent Manager console as an administrator, and open the **Manage Server** window.

3. Click the **LDAP** tab, then the **Add** button.
4. Enter the name of the domain that contains the LDAP or AD server. Users must also enter this domain name when they log into UNIX Agent Manager.
5. Select the domain and provide the information as requested on the window using the following guidelines:
   - In **Server Address**, enter LDAP or Active Directory server computer name and port. For example, `ldap://houston.itservice.production:389`
   - In **User's Parent DN**, enter the path to the node that contains the usernames you want to use. For example, `ou=AMAdmins,dc=netiq,dn=com`
   - In **Username Attribute**, enter the attribute you want UNIX Agent Manager to use to identify the user. This attribute will be used as a consistent identifier even if the user name changes. The default and only attribute supported by UNIX Agent Manager 7.2 is `uid`
   - (Conditional) If you use simple authentication for specific users, in **Username**, enter the path to the user name. For example, `ou=Operator,dc=netiq,dn=com`
6. Click **Save**.

3.5.2 SSL Communication with the LDAP or Active Directory Server

The UNIX Agent Manager server can communicate with the LDAP or Active Directory server using Secure Sockets Layer (SSL). If you choose to have UNIX Agent Manager server communicate with the server using SSL, you must obtain and manage the required certificates. UNIX Agent Manager requires certificates that are base-64 encoded and use the `.cer` extension.

For example, to get a certificate from an OpenLDAP server, run the following command from the `/etc/openldap/certs` directory on the computer that is running the slapd daemon:

```
certutil –L –a –n "OpenLDAP Server" –d `pwd` > servername.pem
```

The command creates a `servername.pem` file that you can import into UNIX Agent Manager using the Manage Server window where you identify your LDAP server.

Ensure you close and restart the UNIX Agent Manager after you import the certificate.

3.6 Restart Methods for the UNIX Agent

NetIQ recommends that you accept the default, rclink. However, the following start methods are available.

Option	Description
`rclink`	Starts the agent daemons immediately after the deployment process and adds a startup script to the `/etc/rc.d` directory. This startup script starts the agent daemons after each reboot when the master rc script runs. This is the default method, and should be used in nearly all environments.
`inittab`	Starts the agent daemons immediately after the deployment process and adds an entry to the `/etc/inittab` file. This inittab file entry starts the agent daemons at the default run level after each reboot.
`inetd`	Configures the (x)inetd daemon to start the agent daemons when needed and then stop and unload the agent daemons.

3.7 Saving UNIX Agent Information to a File

The UNIX Agent Manager server stores the information about the UNIX agents you monitor. However, storing the information to a separate file can be useful for backups or for copying the server to another computer. You can store your UNIX agent list and configuration information in a file outside the UNIX Agent Manager server by clicking **Manage Hosts > Export/Import Host Lists** in UNIX Agent Manager version 7.2.

If you are upgrading from UNIX Agent Manager 7.1 to 7.2, save your configuration information before you upgrade so you can import it after you upgrade. You can export your UNIX agent information from UNIX Agent Manager version 7.1, then import the information into UNIX Agent Manager 7.2.

To export the host information from UNIX Agent Manager 7.1:

1. In the left pane of UNIX Agent Manager 7.1, click **Agent Manager**.
2. Click **Hosts > Edit Hosts**.
3. Select all of the hosts in the Current Hosts list.
4. Click **Export Selected.**

4 Understanding Security Rules

The following section provides an overview of UNIX agent rules and how to implement them using the UNIX Agent Manager. You can access Rules Manager in UNIX Agent Manager by clicking **File** > **Rules Manager**.

4.1 Understanding UNIX Agent Rules

You can protect your information assets and ensure uniform security by applying UNIX agent rule sets. By working in conjunction with the event detection and alerting daemon, rule sets offer real-time event detection, alerting, and response. The default rule set provides a wealth of UNIX knowledge and an excellent starting point from which to build custom rule sets.

UNIX Agent Manager provides a Rule wizard that guides you through creating rules to monitor and react to a number of common conditions, including the following:

- Terminating daemons
- Running specific sensitive commands
- Running sensitive commands in a context other than root
- Creating, modifying, or deleting of specific files

You can deploy the rule sets that you create to any or all of the UNIX computers in your enterprise.

4.2 Understanding Rule Sets

Rule sets are collections of rules you want to enforce on a specific UNIX agent computer or a group of UNIX agent computers. You can create rule sets that are specific to the location, job, or sensitivity of a particular UNIX or Linux computer, or you can easily create a rule set to apply to all your Apache web servers or Oracle database servers. You can enforce unique rule sets on each UNIX agent or deploy a uniform rule set to multiple computers.

Rule set data is normally in a UNIX Agent Manager server, and can be accessed by any UNIX Agent Manager console that is connected to that server. However, you can export the data to a file that can be imported into another server. When you import a rule set, you have the opportunity to change the name of that rule set.

4.2.1 Selecting a Rule Set to Edit

Before you start working with a rule set, determine what rule set you want to modify. Consider the following scenarios:

- Consider reviewing and editing the default rule set provided with the UNIX Agent Manager if this is an initial implementation of rule sets in your organization. The UNIX Agent Manager displays the default rule set when you open Rules Manager. If you modify the default rule set, consider saving the new rule set with a unique name.
- Open a saved rule set if you have already begun to edit a rule set and saved that rule set with a custom name. You might also need to open a saved rule set if you have template rule sets based on the job-related use of the agent computer. For more information, see Section 4.2, "Understanding Rule Sets," on page 29
- Retrieve a rule set from an agent computer if you want to modify the rules enforced on a specific agent computer. For more information, see Section 4.2.4, "Activating Rule Sets on Remote Hosts," on page 31

4.2.2 Viewing Rule Sets and Editing Rule Set Properties

When you open a rule set, the UNIX Agent Manager provides both a tree pane and a list pane. The tree pane provides an easy way to navigate through specific event source and rule group information, while the list pane changes to provide detailed information about your tree selection.

At the second level of the tree, you can find the event sources and rule groups of the rule set. The following list provides a short description of the contents of this secondary tree level and references for more information:

- Event sources provide the data on which to trigger your rules. For more information, see Section 4.5, "Understanding Event Sources," on page 32.
- Rule groups provide editable properties at the group level, and contain individual rules. For more information, see Section 4.6, "Understanding Rule Groups," on page 34.
- Expanding a rule group allows you to view and edit the rules associated with its common event source. For more information, see Section 4.7, "Understanding Rules and Actions," on page 36

UNIX Agent Manager displays disabled rules and event sources in a darker color.

Editing Properties

The content pane allows you to view the configuration of any selected tree element. But, you cannot edit the properties in the content pane.

To edit the properties of an element:

1. Right-click the element in the tree pane. You cannot modify the properties of action elements and conditional elements from the tree pane. For more information, see Section 4.7, "Understanding Rules and Actions," on page 36, Section 4.9, "Understanding Conditionals and Comparisons," on page 38, and Section 4.10, "Understanding Time Conditions," on page 41.
2. Select **Edit** on the menu.
3. On the Edit window, modify the appropriate properties.
4. Click **OK** to save the modifications and close the window.

4.2.3 Saving Rule Sets Locally

After modifying a rule set for a specific agent computer or for a group of agent computers, consider saving the modified rule set to the local computer. Saving a copy of the rule set locally allows you to build an archive of rule sets and saves you the time involved in retrieving rule sets from remote agent computers. To save a copy of the rule set on the UNIX Agent Manager computer, click File > Save or File > Save As, and save the rule set using an .xml extension. If you began with the default rule set, ensure you use the save as option. You cannot save the default rule set with any other name than detect.xml. While the default rule set is write-protected, avoid changing the file attributes and overwriting the default rule set.

4.2.4 Activating Rule Sets on Remote Hosts

Pushing a rule set to an agent computer replaces the previous rule set. The event detection and alerting daemon begins processing and initializing the new rule set immediately. However, it may take up to 30 seconds for the new rule set to take effect. Modifications to items in the filesystem rule group may cause the event detection and alerting daemon may take longer to initialize, due to the time it takes to create initial snapshots of the filesystem objects.

To activate the selected rule set on one or more remote agent computers:

1. Select one or more agent computers in the **Available Hosts** list.
2. Select a rule set.
3. Click **To Selected Hosts**.

4.3 Deciding How to Create UNIX Rules and Rule Sets

UNIX Agent Manager provides both wizard-driven rule creation and the ability to create custom rules not covered by the wizard.

Use the wizard if you want to monitor one or more of the following:

- Rules that trigger when a certain daemon terminates
- Rules that trigger when a log file decreases in size
- Rules that trigger when certain commands are run
- Rules that trigger when certain commands are run by users other than root
- Rules that trigger when certain files are changed or created

To start the wizard, click the **Add Rules** button on the left area of the **Rules Manager** screen, provide a name for the rule set to open the Rules editor, the click **Wizard > Rules Wizard**.

4.4 Using the Rule Wizard to Create Rules

The Rule wizard helps you quickly create the following types of rules:

- Rules that trigger when a certain daemon terminates
- Rules that trigger when a log file decreases in size
- Rules that trigger when certain commands are run
- Rules that trigger when certain commands are run by users other than root
- Rules that trigger when certain files are changed or created

To use the Rules Wizard to create rules:

1. Click **Wizard > Rule Wizard** to start the Rule wizard.
2. On the select rule type window, select the appropriate rule type, and then click **Next**. For more information, see the description of rule type or Section 4.7, "Understanding Rules and Actions," on page 36.
3. On the Rule Description window, provide a name for the rule, and then click **Next**.
4. On the Rule Name window, provide a descriptive name for the rule, and then click **Next**.
5. ***If you are using the Log_file_shrunk or modified_file rule,*** select either **Names** or **Paths**, and then click **Next**. Selecting **Name** causes the event detection and alerting daemon to monitor all files with a certain name. Selecting **Paths** causes the event detection and alerting daemon to monitor a specific file.
6. On the Name of File window, specify the name of the object you want to monitor and click **Next**. The name depends on the rule type selected, which might be a daemon executable, a command, a file name, or a fully-qualified path. For example, if you selected **Paths** while creating a modified_file rule, specify the full path, including the file name you want to monitor.
7. Provide the appropriate information for the action you want the rule to trigger in response to an event, and then click **Next**. All fields are optional. You do not need to select an action to create a rule. For more information, see Section 4.7, "Understanding Rules and Actions," on page 36
8. Review the information provided about the rule group associated with your rule, and then click **Next**.
9. Complete the Rule wizard. The Rule wizard displays only the windows relevant to the event source you associated with the new rule. If the new rule is in a rule group that uses configurable event sources, the remaining windows offer you the ability to modify the configurable parameters. Read the descriptions provided and, if necessary, modify parameters. If you are unsure, retain the current value.
10. When you have completed the Rule wizard, click **Finish**.

4.5 Understanding Event Sources

Event sources extract a particular type or class of events from one of the following providers:

- Operating system
- Daemon
- Server
- Application

Typically, event sources extract the required information by parsing and filtering log entries. Once extracted, the log entry is considered an event. All events must be composed of output parameters that can be evaluated by the event detection and alerting daemon.

When an event source detects an event and assigns output parameter values, the event detection and alerting daemon uses the values to trigger the appropriate rule response in the associated rule group. For example, you can configure a rule in an agent computer rule set that alerts you when an FTP event associated with a particular user account is detected. To successfully trigger your FTP rule, you must have an event source that can do the following:

- Monitor the `wtmp` log file, the log in which FTP events are reported
- Parse the log entries
- Generate output about each event

UNIX Agent Manager provides a wtmp event source with the default rule set. This event source scans the wtmp log and generates output about each entry in the log. The wtmp event source extracts a number of properties, including the event type and user login name, and provides them to the event detection and alerting daemon. Specifically, the event type and user login are defined as the $id and $user output parameters. If the value of an output parameter matches criteria you configure in a rule, the actions you specify in the rule properties trigger.

You can use a single event source for multiple rule groups, but consider configuring each event source to monitor unique log files. Configuring multiple rule groups to use identical event sources and setting configuration parameters to the same values, is undesirable. You duplicate the monitoring, parsing, and output parameter generation between instances of the event source. You specify the event source of a rule group by editing the properties of its corresponding rule group. For more information, see Section 4.6.1, “Editing Rule Group Properties,” on page 34.

4.5.1 Editing Event Source Properties

The UNIX Agent Manager provides the ability to edit existing event source properties. Ensure you fully understand the purpose and capabilities required of an event source before editing currently functioning event sources. For more information, see Section 4.5, “Understanding Event Sources,” on page 32.

To edit event source properties:

1. Right-click the event source that you want to edit.
2. Click **Edit**.
3. On the Edit Event Source window, select the tab of the properties you want to modify.
4. Modify the property, and then click **OK**.

4.5.2 Creating New Event Sources

The UNIX Agent Manager provides the ability to create your own event sources. Ensure you fully understand the purpose and capabilities required of an event source before attempting to create an event source. For more information, see Section 4.5, “Understanding Event Sources,” on page 32.

To create new event sources:

1. Right-click the Rule Set node in the tree area, and then click **Add Event Source**.
2. Configure the event source properties in the Add Event Source window, and then click **OK**. For examples of syntax, view the properties of an existing events source in the default rule set.

After configuring an event source, you can create a rule group associated with the event source. For more information, see Section 4.6.2, “Creating New Rule Groups,” on page 34.

4.5.3 Deleting Event Sources

The UNIX Agent Manager provides the ability to delete existing event sources. Ensure you fully understand the purpose of an event source before deleting the event source. For more information, see Section 4.5, “Understanding Event Sources,” on page 32.

To delete an event source from a rule set:

1. Delete all rule groups associated with the event source or reconfigure the rule groups to use a different event source. For more information, see Section 4.6.3, “Deleting Rule Groups,” on page 35 and Section 4.6.1, “Editing Rule Group Properties,” on page 34.
2. Right-click the event source that you want to delete, and then click **Delete**.
3. Click **Yes** on the Delete window.

After deleting an event source, you can save the modified rule set on the UNIX Agent Manager computer and activate the modified rule set on remote agent computers. For more information, see Section 4.2.3, “Saving Rule Sets Locally,” on page 31 and Section 4.2.4, “Activating Rule Sets on Remote Hosts,” on page 31.

4.6 Understanding Rule Groups

Rule groups contain one or more rules sharing common event sources, schedules, and other properties. Clicking a rule group in the tree area displays the group properties in the content area. Rule group properties consist of the following information:

- Delay
- Event source name
- Event source parameters for the rules contained in the rule group
- Name and description of the rule group
- Nice value or process priority

Increasing the allowable delay and nice value lowers the impact on the resources of the agent computer.

4.6.1 Editing Rule Group Properties

You can easily edit the properties of a rule group. Consider editing rule group properties to change the name or description of a rule group or to lessen the resource impact of executing the rules contained in the rule group.

To edit rule group properties:

1. Right-click the rule group you want to edit, and then click **Edit**.
2. Modify the rule group properties on the Edit Group window, and then click **OK**.

4.6.2 Creating New Rule Groups

You can create two different types of rule groups:

- Real-time rule groups
- Scheduled rule groups

Real-time Rule Groups

Real-time rule groups detect events and evaluate rules as the events occur.

To create real-time rule groups:

1. Use an existing event source or create a new event source for the new rule group. For more information, see Section 4.6.1, "Editing Rule Group Properties," on page 34.
2. Right-click **Rule Set**, and then click **Add Real-time Group**.
3. On the Add Real-time Group window, configure the rule group properties, and then click **OK**.

After configuring a real-time rule group, you can create rules in the rule group that detect events as they occur. For information about creating rules and actions, see Section 4.7.2, "Creating New Rules and Actions," on page 37.

Creating Scheduled Rule Groups

Scheduled rule groups detect events and evaluate rules during scheduled times. You can schedule rules to activate for minute-long increments during any number of minutes in a year.

To create scheduled rule groups:

1. Right-click **Rule Set**, and then click **Add Scheduled Group**.
2. On the Add Scheduled Group window, configure the properties of the rule group. You can edit values by typing in the fields. To declare more than one value in a scheduling attribute, separate the values with commas.
3. Click **OK** to close the window.

After configuring a scheduled rule group, you must create rules in the rule group. All rules contained in the scheduled rule group have identical schedules. For information about creating rules and actions, see Section 4.7.2, "Creating New Rules and Actions," on page 37.

4.6.3 Deleting Rule Groups

If you no longer need a rule group, you can delete it. Before deleting a rule group, consider making a backup copy of the rule set. By backing up your rule set, you ensure you do not lose rules and rule groups you may want to reactivate in the future. Deleting a rule group also deletes the rules it contains.

To delete a rule group and all of the rules it contains from a rule set:

1. Right-click the rule group that you want to delete, and then click **Delete**.
2. On the Delete window, click **Yes**.

After deleting a rule group, if you no longer need the associated event source for other rule groups, you can delete the associated event source. Save the modified rule set on the UNIX Agent Manager computer and activate the modified rule set on remote agent computers. For more information, see Section 4.2.3, "Saving Rule Sets Locally," on page 31 and Section 4.2.4, "Activating Rule Sets on Remote Hosts," on page 31.

4.7 Understanding Rules and Actions

Rules contain all of the information the event detection and alerting daemon needs to evaluate event source output parameters and trigger actions. Expanding a rule group displays the rules contained in the rule group. Rules that appear in the same group have common event sources and schedules, if applicable.

A rule is defined and governed by one or more of the following properties:

- Actions.
- Initialization code. For more information, see Section 4.8, "Understanding Initialization Code," on page 38.
- Main code. For more information, see Section 4.11, "Understanding Main Code," on page 42.
- Conditionals -- And and Or objects. For more information, see Section 4.9, "Understanding Conditionals and Comparisons," on page 38.
- Comparisons. For more information, see Section 4.9, "Understanding Conditionals and Comparisons," on page 38.
- Time conditions. For more information, see Section 4.10, "Understanding Time Conditions," on page 41.
- Templates contain information for the Rule wizard. Template nodes do not require user maintenance.

The UNIX Agent Manager displays these properties as child objects of the rule in the tree. The following figure illustrates the tree arrangement of the default telnet rule.

Actions are the responses available for a detected event. The following definitions provide more information about your options:

E-mail

Specifies the name, e-mail address, and message content you want sent when the rule triggers. Populate these fields with the appropriate information. Separate multiple e-mail addresses with a comma (,). You must have sendmail configured correctly on the agent computer to send e-mail.

SNMP Message

Specifies the SNMP message you want sent when the rule triggers. Select the appropriate notification for this field.

Log

Specifies the name of the log file and the message written in the log file when the rule triggers. Provide the appropriate information in these fields.

Command

Specifies a Bourne shell command to execute on the agent computer when the rule triggers. Provide an appropriate command in this field.

Security Manager Event

Specifies the NetIQ classification attribute used to classify events for Log Manager.

4.7.1 Viewing and Editing Rule Properties and Actions

Clicking a rule displays the properties, configuration, actions, conditions, and advanced settings of the rule in the content pane. The rule attributes tab identifies and describes the rule; the configuration tab displays the rule configuration; the actions tab specifies the actions to perform when the rule triggers; the conditions tab displays the conditions that must be met for the rule to trigger; and the advanced tab displays the rule debug level.

Expanding an action node displays a sub-node that is labeled with the action that will occur if the rule triggers. For example, an element that is labeled `Alert: $user logged in at $time` describes the alert message that displays when the rule triggers.

To edit existing rule properties:

1. Right-click the rule that you want to edit, and then click **Edit**.
2. On the Edit Rule window, modify the appropriate rule properties, and then click **OK**.

NOTE: Use only Bourne shell commands when specifying Command rule properties.

4.7.2 Creating New Rules and Actions

Creating new rules can be a time consuming task. Before creating new rules, ensure you have investigated the following statements are true:

- You cannot use the Rules wizard.
- You cannot find an existing rule to modify.

To create new rules and actions in a rule group:

1. Right-click a rule group that is associated with the event source that you want to use, and then click **Add Rule**.
2. On the Add Rule window, configure the appropriate rule group properties and actions, then click **OK**.

NOTE: Use only Bourne shell commands in the Command attribute.

After configuring the rule, you can save the modified rule set on the UNIX Agent Manager computer and activate the modified rule set on remote agent computers. For more information, see Section 4.2.3, “Saving Rule Sets Locally,” on page 31 and Section 4.2.4, “Activating Rule Sets on Remote Hosts,” on page 31.

4.7.3 Deleting Rules and Actions

If a rule and its associated actions are no longer necessary in your environment, consider deleting the rule and its actions. Consider making a backup of the rule set before deleting rules.

To delete a rule and its associated actions from a rule set:

1. Right-click the rule that you want to delete, and then click **Delete**.
2. Click **Yes** on the Delete window.

After deleting a rule and its associated actions, you can save the modified rule set on the UNIX Agent Manager computer and activate the modified rule set on remote agent computers. For more information, see Section 4.2.3, “Saving Rule Sets Locally,” on page 31“Saving Rule Sets Locally” and Section 4.2.4, “Activating Rule Sets on Remote Hosts,” on page 31.

4.8 Understanding Initialization Code

Initialization code, written in Perl, runs when the rule set is activated. Your rule requires initialization code if it relies on parameters or tables not previously configured. If the rule configures itself through querying the operating system or daemons, the rule requires initialization code. Rule containing initialization code display Init Code as a child element in the tree pane.

4.8.1 Viewing and Editing Initialization Code

To view initialization code, expand the appropriate rule, and then click Init Code. Review the initialization code in the content pane.

Complete the following procedure to edit existing rule initialization code.

To edit existing initialization code:

1. Right-click **Init Code**, and then click **Edit**.
2. Modify the Perl code in the Edit Initialization Code window that opens, and then click **OK** to close the window.

4.8.2 Adding New Initialization Code

Complete the following procedure to add new initialization code to a rule.

1. Right-click the rule you want to modify, and then click **Add Initialization Code**. You can add one set of initialization code per rule.
2. On the Edit Initialization Code window, add the appropriate Perl code, and then click **OK**.

4.8.3 Deleting Initialization Code

If you no longer need the initialization code for a rule, you can delete the code. Consider making a backup of the rule set before deleting rules.

To delete initialization code:

1. Ensure the rule does not have parameters or tables that require the initialization code.
2. Right-click the initialization code you want to delete, and then click **Delete**.
3. On the Delete window, click **Yes**.

4.9 Understanding Conditionals and Comparisons

You declare conditionals and comparisons to ensure you trigger actions only when necessary. Conditionals and comparisons help you filter event source output parameters. Consider the following example from the telnet rule:

- `$message =~ /telnet/`
- `$source =~ /telnet/`

Because you can find these entries in an Or child element of the telnet login rule, you know the rule triggers when any one of the comparisons is true. When the syslog event source generates a $message or a $source parameter equivalent to telnet, the event detection and alerting daemon searches the output parameters and triggers the defined actions.

To trigger an action when both comparisons are met, you create And comparisons. And comparisons trigger rule actions when both comparisons evaluate as true.

The hierarchy of the tree graphically represents the order in which conditional and comparison expressions are evaluated. While the tree displays one conditional or comparison under the rule element, the And or Or may have numerous child elements. Rules that do not have conditional or comparison statements must have main code to trigger. For more information, see Section 4.11, "Understanding Main Code," on page 42.

Rules that contain a comparison not as a child element of an And or Or comparison is not a conditional. These comparisons trigger actions when the event detection and alerting daemon evaluates the statement as true.

4.9.1 Viewing and Editing Comparison Properties

You can view the properties of a comparison by clicking the comparison in the tree pane and viewing properties in the content pane. Comparisons are labeled with the output parameter name, equation, and value describing the comparison. For example, `$message =~ /telnet/`.

You can edit comparison properties by completing the following procedure.

To edit existing comparison properties:

1. Expand the appropriate rule.
2. Right-click the comparison you want to edit, and then click **Edit**.
3. On the Edit Comparison window, modify the comparison properties, and then click **OK**.

NOTE: When defining the Value property, enclose regular expressions with slashes (/) to indicate that the value is a regular expression. For example, `/telnet/` designates telnet is a regular expression.

After modifying the properties of the comparison, you can save the modified rule set on the UNIX Agent Manager computer and activate the modified rule set on remote agent computers. For more information, see Section 4.2.3, "Saving Rule Sets Locally," on page 31 and Section 4.2.4, "Activating Rule Sets on Remote Hosts," on page 31.

4.9.2 Adding Comparisons

The following procedure guides you through adding comparisons to a rule.

To add comparisons:

1. ***If you want to associate a comparison with a conditional,*** you must first add the conditional. For more information, see Section 4.9.3, "Adding And," on page 40, Section 4.9.4, "Adding Or," on page 40, and Section 4.9.5, "Associating Comparisons with Conditionals," on page 40.
2. (Conditional) If you want to add a new comparison that is not associated with a conditional, right-click the rule you want to modify, and then click **Add Comparison**.
3. On the Add Comparison window, configure comparison properties, and then click **OK**.

NOTE: When defining the Value property, enclose regular expressions with slashes (/) to indicate that the value is a regular expression. For example, `/telnet/` designates telnet is a regular expression.

After adding comparisons to a rule, you can save the modified rule set on the UNIX Agent Manager computer and activate the modified rule set on remote agent computers. For more information, see Section 4.2.3, "Saving Rule Sets Locally," on page 31 and Section 4.2.4, "Activating Rule Sets on Remote Hosts," on page 31.

4.9.3 Adding And

And conditionals declare that all the conditional components must be true for the actions of a rule to trigger. The following procedure guides you through adding And conditionals to your rule.

To add and conditionals:

1. (Conditional) If you want to trigger actions when all comparisons in a group of comparisons evaluates as true, right-click the rule you want to modify, and then click **Add And**.

   NOTE: The tree pane displays only one conditional or comparison as a child element of the rule in the tree pane. You can nest And conditionals within other conditionals. To do nest conditionals, right-click the conditional, and then click **Add And**.

2. Add comparisons as child elements to the conditional. For more information, see Section 4.9.5, "Associating Comparisons with Conditionals," on page 40.

4.9.4 Adding Or

Or conditions declare that any one of the conditional components must be true for the actions of a rule to trigger. The following procedure guides you through adding Or conditionals to your rule.

To add or conditionals:

1. (Conditional) If you want to trigger actions when any comparison in a group of comparisons evaluates as true, right-click the rule that you want to modify, and then select **Add Or** from the pop-up menu.

   NOTE: The tree pane displays only one conditional or comparison as a child element of the rule in the tree pane. You can nest And conditionals within other conditionals. To do nest conditionals, right-click the conditional, and then click **Add Or**.

2. Add comparisons as child elements to the conditional. For more information, see Section 4.9.5, "Associating Comparisons with Conditionals," on page 40.

4.9.5 Associating Comparisons with Conditionals

You can associate two or more comparisons with a conditional. The UNIX Agent Manager displays comparisons you associate with a conditional as child elements of the conditional. Complete the following procedure to associate comparisons with a conditional.

To associate comparisons with a conditional:

1. Right-click the conditional, and then click **Add Comparison**.
2. On the Add Comparison window, configure comparison properties, and then click **OK**.

   NOTE: When defining the Value property, enclose regular expressions with slashes (/) to indicate that the value is a regular expression. For example, `/telnet/` designates telnet is a regular expression.

After associating comparisons with conditionals in a a rule, you can save the modified rule set on the UNIX Agent Manager computer and activate the modified rule set on remote agent computers. For more information, see Section 4.2.3, "Saving Rule Sets Locally," on page 31 and Section 4.2.4, "Activating Rule Sets on Remote Hosts," on page 31.

4.9.6 Deleting Comparisons or Conditionals

When you no longer need a comparison or a conditional, you can delete it from the rule set. Ensure you no longer need the comparison or conditional to trigger your rule actions. Complete the following procedure to delete a comparison or conditional.

To delete a comparison or a conditional and the associated comparisons and nested conditionals:

1. In the tree pane, right-click the comparison or the conditional you want to delete, and then click **Delete**.
2. On the Delete window, click **Yes**.

After deleting the comparisons or conditionals, you can save the modified rule set on the UNIX Agent Manager computer and activate the modified rule set on remote agent computers. For more information, see Section 4.2.3, "Saving Rule Sets Locally," on page 31 and Section 4.2.4, "Activating Rule Sets on Remote Hosts," on page 31.

4.10 Understanding Time Conditions

Time conditions allow you to specify when you want a rule activated and ready to trigger. A time condition specifies the days and hours during the week when you want to activate the rule. For example, if your information security policy does not allow FTP sessions after hours, you can attach a time condition to the FTP rule that alerts you only when FTP sessions initiate after hours.

4.10.1 Viewing and Editing Time Conditions

To view time conditions, expand the rule containing the time condition, and then click **Time Condition**. The UNIX Agent Manager displays when the associated rule is active.

If you want to change the schedule of a rule governed by a time condition, complete the following procedure.

To edit existing time conditions:

1. Right-click the time condition that you want to edit, and then click **Edit**.
2. Select the days and hours on which you want to activate the rule. You can use the `Ctrl` and `Shift` keys to select multiple days and times.
3. Click **OK**.

4.10.2 Adding New Time Conditions

The following procedure guides you through adding a time condition to a rule. You can designate one time condition per rule. Time conditions ensure rules only run when necessary.

To add a new time condition:

1. Right-click the rule that you want to modify, and then click **Add Time Condition**.
2. Select the days and hours on which you want to activate the rule. You can use the `Ctrl` and `Shift` keys to select multiple days and times.
3. Click **OK**.

4.10.3 Deleting Time Conditions

You can remove time conditions and have a rule active all the time. Complete the following procedure to delete a time condition.

To delete time conditions:

1. Right-click the time condition node you want to delete, and then click **Delete**.
2. On the Delete window, click **Yes**.

4.11 Understanding Main Code

Main code is Perl code you can add to a rule if the filtering provided by the conditionals and comparisons is inadequate or needs augmenting to detect more complex patterns. Main code must contain a call to the subroutine `_take_actions()`. The code you write can be selective about the circumstances under which the subroutine is called. It is not necessary for the code to call `_take_actions()` every time it is evaluated. Rule that contain main code display the Code element in the rule.

4.11.1 Viewing and Editing Main Code

To view main code, expand the rule containing the main code you want to view, and then click **Code**.

The UNIX Agent Manager also allows you to edit existing main code. Before editing code that functions correctly, ensure you make a back up of the rule set. Complete the following procedure to edit your main code.

To edit existing main code:

1. Expand the appropriate rule, and then right-click **Code**.
2. Click **Edit**.
3. On the Edit Code window, modify the Perl code.
4. Click **OK**.

After editing main code, you can save the modified rule set on the UNIX Agent Manager computer and activate the modified rule set on remote agent computers. For more information, see Section 4.2.3, “Saving Rule Sets Locally,” on page 31 and Section 4.2.4, “Activating Rule Sets on Remote Hosts,” on page 31.

4.11.2 Adding New Main Code

The UNIX Agent Manager allows you to add main code to a rule. Before adding main code, ensure you have a thorough knowledge of Perl and a complete understanding of what you want the code to accomplish. You can create one set of main code per rule.

To add main code:

1. Right-click the rule to which you want to add main code, and then click **Add Main Code**.
2. On the Edit Code window, add your Perl code.
3. Click **OK**.

After adding new main code, you can save the modified rule set on the UNIX Agent Manager computer and activate the modified rule set on remote agent computers. For more information, see Section 4.2.3, "Saving Rule Sets Locally," on page 31 and Section 4.2.4, "Activating Rule Sets on Remote Hosts," on page 31.

4.11.3 Deleting Main Code

Before deleting main code, ensure you no longer need the code to make the rule work. Complete the following procedure to delete main code.

To delete main code:

1. Right-click the main code you want to delete, and then click **Delete**.
2. On the Delete window, click **Yes**.

4.12 Customizing the Rules Management User Interface

The UNIX Agent Manager provides a number of options that allow you to adjust the appearance and usability rules management. The following sections provide overviews of the features you can select from the **Customize** menu.

4.12.1 Deciding Whether to Use Tabbed Layouts

Tabbed layouts allow you to select how you want to view configuration information in the content area. The following figure illustrates the default tabbed layout of the filesystem event source. The tabbed layout provides easy to read information grouped into specific categories. You navigate to other configuration categories by clicking the corresponding tab.

The following figure shows the same event source displayed without the category grouped tabs. The non-tabbed layout option shows all the configuration information in one pane. This option is convenient if you have a large monitor and want to see all the information about an element. The pane borders are adjustable so that you can show more or less of each section. To adjust the pane border, click the border and drag it up or down.

4.12.2 Deciding Whether to Use Parameter Aliases

The UNIX Agent Manager uses parameter aliases to make parameters generated by event sources or rules easier to understand. The UNIX Agent Manager provides parameter aliases to make the configuration of alerts easier. Aliases are more descriptive than the actual parameter names.

For example, if parameter aliases are turned off, an alert message in the configuration area may look like the following:

```
Linux user, $user, logged in via ftp at $time, from $host at @addr_linux.
```

However, with parameter aliases turned on, the same alert message is easier to understand:

```
Linux user, (User name), logged in via ftp at (Hour:Minute:Second) from (Remote
host name) at (Linux remote host Internet address).
```

Aliases are enclosed in parenthesis to visually sets them apart from the surrounding text.

When you configure rules using the descriptive aliases instead of the parameter name, the UNIX Agent Manager Rules Manager automatically substitutes the appropriate parameter. You can view the parameters, their associated aliases, and a description of their functions in the event source configuration area Output tab.