NetIQ® Security Agent for UNIX

Installation and Configuration Guide

November 2016

Legal Notice

Contents

About this Book and the Library

This book provides steps for UNIX Agent Manager (UAM) installation, steps for Security Agent for UNIX (Agent) deployment, and integration information for the NetIQ Change Guardian (Change Guardian), the NetIQ Sentinel (Sentinel), and NetIQ Secure Configuration Manager (Secure Configuration Manager) products. This book defines terminology and includes implementation scenarios.

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.

1 Understanding Security Agent for UNIX

Securing and monitoring performance of your UNIX and Linux environments can be expensive and time-consuming. The following are the most common issues that enterprise performance and security managers experience:

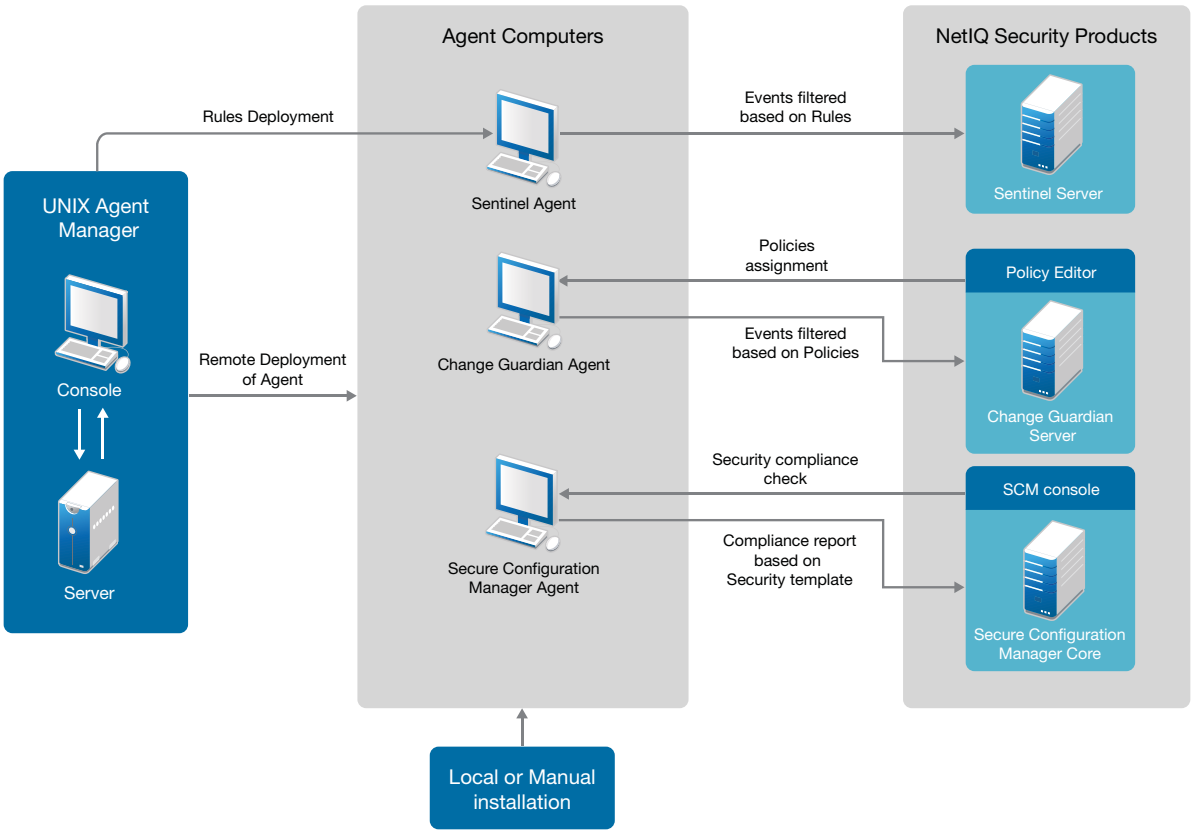
- Deficits in staff knowledge concerning UNIX and Linux security and system expertise
- Managing various operating systems including Red Hat, AIX, HP-UX, Solaris, and SUSE Linux
- Controlling access to privileged commands and sensitive resources
- Lacking intrusion detection and response systems to handle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

The Security Agent for UNIX (Agent) helps you effectively address these challenges by enabling NetIQ security products, such as Secure Configuration Manager, Change Guardian, and Sentinel, to monitor the configuration and risk compliance of your UNIX and Linux environments.

The Agent validates the configuration of UNIX and Linux endpoints to ensure that compliance with corporate security policies and find potential vulnerabilities. An endpoint represents an Agent-monitored operating system, application, web server, or database instance.

It collects security compliance information from one or more endpoints in one or many domains. The Agent receives requests from NetIQ security products and runs commands or responds by returning data, status, or results. It runs locally on computers throughout your enterprise.

Figure 1-1 *Security Agent for UNIX Architecture*



NetIQ UNIX Agent Manager is a console that you can use to manage all your 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 allows you to install and configure all your Agent components across your enterprise instead of interacting with the Agents individually. UNIX Agent Manager also allows you to see any UNIX computers that Secure Configuration Manager, Sentinel, and Change Guardian monitor. UNIX Agent Manager consists of 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.

The Agent communicates with the UNIX Agent Manager server. The user can install, upgrade, stop, and start the Agent through a command line interface or through the UNIX Agent Manager console. UNIX Agent Manager server communicates with the main NetIQ security products. The server stores information about where the Agents are installed, where consoles are installed, and which users have access to change what information about the Agents. The user need not interact directly with the UNIX Agent Manager Server. Users can use the UNIX Agent Manager console to install, configure, patch, monitor, start, and stop the Agents across their enterprise.

When you install an Agent, you can choose which NetIQ security products (Sentinel, Change Guardian, or Secure Configuration Manager) will monitor the computer on which the Agent resides. A single Agent can perform monitoring for one or more NetIQ security products. Each NetIQ security product has its own method for registering the Agents and configuring the Agent to send the proper data.

Each Agent sends regular communication, called a heartbeat, to verify the operation. When the Agent receives a heartbeat request, the Agent polls its monitored endpoints to verify their statuses and then responds to NetIQ security products.

For Sentinel, the rules are deployed on the Sentinel Agent via UNIX Agent Manager. The events are filtered and forwarded to the Sentinel server based on the rules deployed. You can monitor the most complex IT environments and obtain the security required to protect your IT environment.

For Change Guardian, the policies are deployed to monitor critical files on Change Guardian Agent via policy editor. The events are filtered and forwarded to the Change Guardian server based on the policies assigned. You can monitor security event details that pinpoint the who, what, when, where, and authorization status of a change or activity, including before and after details of the change.

For Secure Configuration Manager, the Agent also responds to requests for data sent from core services in the form of security checks and policy templates. Policy templates are groups of security checks to audit a specific series of IT controls that match a security policy standard. The Agent translates the security checks into queries and forwards to its monitored endpoints. Upon receiving responses to the queries, the Agent reports the results to the Secure Configuration Manager server.

2 Planning Your Security Agent for UNIX Installation

This chapter provides information about planning the Agent installation. This chapter assumes that you have Sentinel, Secure Configuration Manager, or Change Guardian installed on your computer.

Implementation Checklist

Use the following checklist to plan and install Security Agent for UNIX.

❑	Assess your environment to determine the hardware configuration. Ensure that the computers on which you install Security Agent for UNIX meet the specified requirements. For more information, see "System Requirements" on page 16.
❑	Install the NetIQ security product you want to use with the Agent. If you are using Sentinel, install the Agent Manager Connector also.
❑	Install UNIX Agent Manager. For more information, see Agent"Installing UNIX Agent Manager" on page 21.
❑	Install the Agent on the computer you want to monitor. ◆ For information about remote deployment of the Agent on one or more endpoints, see "Remote Installation Using UNIX Agent Manager" on page 23. ◆ For information about deploying the Agent directly on the endpoint, see "Local Installation" on page 25. ◆ For information about installing using an answer file, see "Silent Installation" on page 25.
❑	Ensure that the audit service is running on the Agent without any interruption. For more information see, "Validating Agent Services Installation" on page 67.
❑	Deploy Sentinel rules using UNIX Agent Manager on the endpoint that helps you to route the parsed event data according to the rules you define. For information about how to deploy rules, see "Deploying Rule Sets" on page 41.

Understanding License Information

This section provides licensing information for NetIQ Security Products that work with Security Agent for UNIX.

- Security Agent for UNIX does not require its own license or license key. The license key and licensing terms are determined by the NetIQ security product monitoring the Agent. You must ensure that the licenses provide the appropriate coverage for your requirements. For more information, see respective product documentation on NetIQ Documentation website.
- Security Agent for UNIX with Secure Configuration Manager does not require licensing separately because the Secure Configuration Manager license is sufficient.
- Security Agent for UNIX with Sentinel does not require licensing separately because the Sentinel license is sufficient.
- Security Agent for UNIX with requires a valid Change Guardian license key and licensing for the Change Guardian for UNIX module.

System Requirements

For information about the recommended hardware, supported operating systems, browsers, and systems monitored by the Agent, see Technical Information for Security Agent for UNIX.

Understanding FIPS 140-2 Implementation

NetIQ security products support Federal Information Processing Standard (FIPS) 140-2 communication among the product components. You can configure the UNIX Agent manager, Security Agent for UNIX, and the NetIQ security products (Sentinel, Change Guardian, and Secure Configuration Manager) to enable all communications to FIPS 140-2 validated cryptographic modules. When you configure them to use only these communication algorithms, the servers cannot fully communicate with any Agent that does not use these algorithms.

The Security Agent for UNIX uses OpenSSL libraries for its internal encryption and other functions. OpenSSL is a FIPS 140-2 validated cryptographic provider. The purpose of doing so is to ensure that the Agent is in FIPS mode and is compliant with United States federal purchasing policies and standards.

UNIX Agent Manager uses Mozilla NSS libraries and Java SSL libraries for creating the listener on port 2222 and OpenSSL libraries for communicating with Agents. For UNIX Agent Manager, we ship our own copies of the Mozilla NSS libraries. Red Hat Enterprise Linux (RHEL) and SUSE Linux Enterprise Server (SLES) have a different set of NSS packages. The NSS cryptographic module provided by RHEL and SLES are FIPS 140-2 validated.

IMPORTANT: If you deploy the Agent in FIPS mode, you must deploy the NetIQ security products in FIPS mode. If not, you can deploy all the components in non-FIPS mode.

Installation Options

The following are different ways in which you can implement FIPS 140-2:

NOTE: If you have converted the Agent to FIPS mode, you cannot revert back to non-FIPS mode.

Tasks	For more information, see…
Local installation: To enable the Agent in FIPS 140-2 mode during local installation	Local installation (page 25)
Remote installation: To enable the Agent in FIPS 140-2 mode during remote installation	Remote installation (page 23)

FIPS-Enabled Components

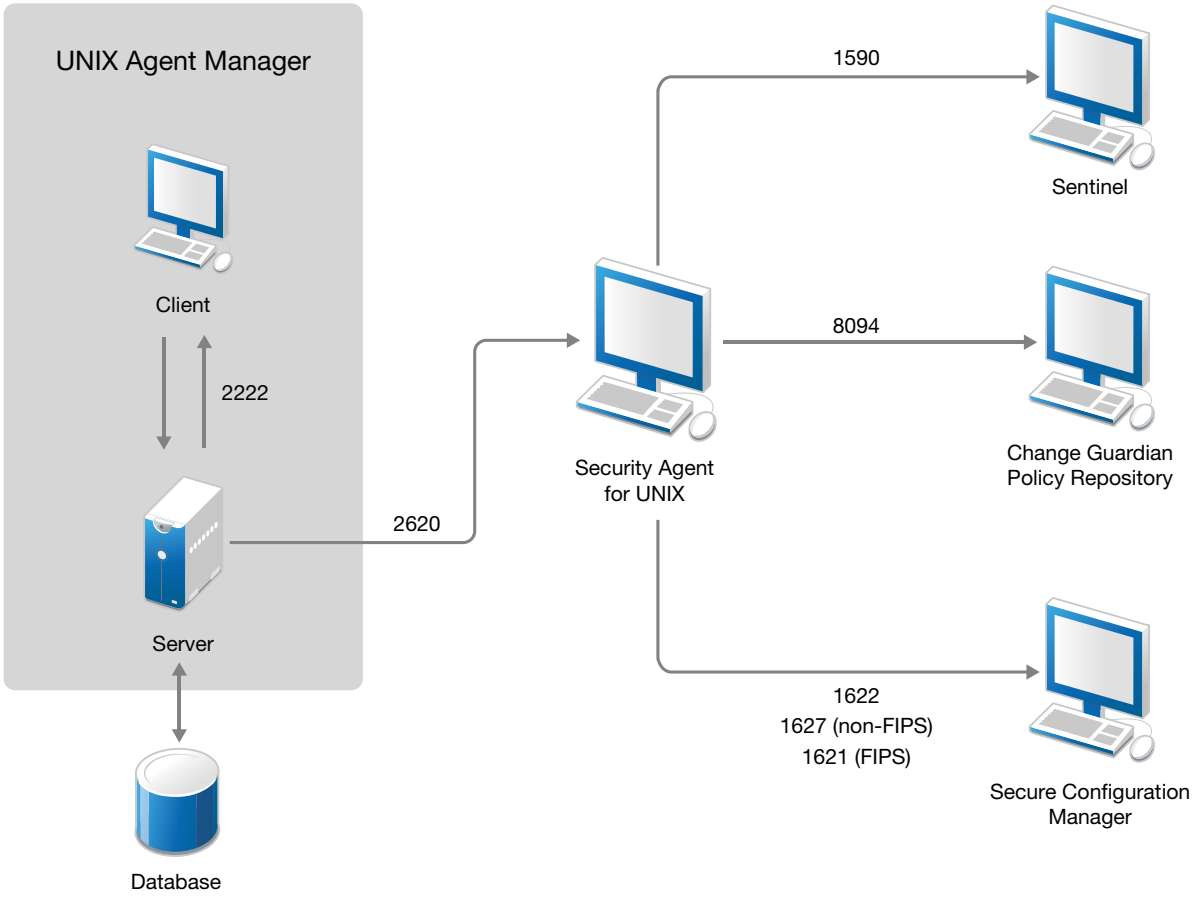
The following components provide FIPS 140-2 support:

- Sentinel Server 7.4 and later
- Change Guardian Server 4.2.1
- Secure Configuration Manager Core 6.1 and later
- Sentinel Security Agent for UNIX 7.5
- Change Guardian Security Agent for UNIX 7.5
- Secure Configuration Manager Security Agent for UNIX 7.5
- UNIX Agent Manager 7.5
- Sentinel Agent Manager Connector 2011.1r5

Ports Used

Security Agent for UNIX uses various ports for external communication with other components. The following figure illustrates the ports used:

Figure 2-1 Ports Used



Port	Description
2620	Communication with UNIX Agent Manager
1590	Communication with Sentinel
8094	Communication with Change Guardian Policy Repository
1622	Communication with Secure Configuration Manager
1627	Communication with Secure Configuration Manager in non-FIPS mode
1621	Communication with Secure Configuration Manager in FIPS mode
2222	Communication between UNIX Agent Manager client and UNIX Agent Manager server

Installation Options

This topic provides information about the various ways to install Security Agent for UNIX:

- Remote deployment using UNIX Agent Manager: Remote deployment provides a convenient and uniform method for installing one or more Agents. You can use the Deployment wizard provided in the UNIX Agent Manager for remote deployment.
- Local installation using command line: Local installation guides you through logging on to an Agent computer and locally installing all required components on the Agent computer.
- Silent installation using answer file: Silent installation allows you to install the Agent without interactively running the installation script. Silent installation uses an installation file that records the information required for completing the installation.

3 Installing Security Agent for UNIX

The Agent installation installs the following components on the Agent computers:

- **UNIX Agent Manager**: A user interface that you can use to manage all your Agent components across your enterprise. UNIX Agent Manager runs on Windows and Linux operating systems. UNIX Agent Manager runs on Linux when a desktop or supported X11 server libraries are installed. 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.
- **Security Agent for UNIX**: A component that enables support for the NetIQ security products.

The following table provides an overview of the tasks required to install the Agent:

Task	See...
Install the UNIX Agent Manager Server.	Installing UNIX Agent Manager (page 21)
Install the UNIX Agent Manager Console on the endpoints where you want to monitor Agents.	Installing UNIX Agent Manager Console (page 21)
Install the Agent on the UNIX and Linux endpoints you want to manage.	Installing the Agent on UNIX and Linux computers (page 23)
Understanding FIPS implementation	"Understanding FIPS 140-2 Implementation" on page 16

Installing UNIX Agent Manager

UNIX Agent Manager is a console used to manage all components across your enterprise. You can use UNIX Agent Manager to install the Agent on several computers at the same time.

After you have installed UNIX Agent Manager, you can set up users and assign access to them. For more information about managing UNIX Agent Manager users, see Chapter 4, "Managing Users Using UNIX Agent Manager," on page 29. The following sections guide you through installing UNIX Agent Manager:

- "Installing UNIX Agent Manager on Microsoft Windows" on page 21
- "Installing UNIX Agent Manager on Linux" on page 22

Installing UNIX Agent Manager on Microsoft Windows

Complete the following steps to install 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. Download and run `UAMInstaller.MSI` from the package in the root folder of the installation kit and continue with the installation as prompted.

NOTE: Do not restrict communication security settings to Federal Information Processing Standard (FIPS) encrypted algorithms unless you are certain that your environment requires that restriction. If you enable FIPS 140-2 mode, UNIX Agent Manager cannot communicate with Agents that are running in non-FIPS mode. For more information about FIPS and the other security level options, see Chapter 5, “Converting Agent from Non-FIPS to FIPS mode,” on page 31.

3 Complete the automatic installer wizard.

4 Specify and confirm a password for the UNIX Agent Manager server. The administrator user account must use this password.

NOTE: To change the administrative password for the UNIX Agent Manager server, start the server using the old password and then reset it in **Manage Server** window by clicking **Reset Admin Password**.

5 Continue with the installation as prompted until the installation is complete.

Installing UNIX Agent Manager on Linux

Complete the following steps to install 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 Download the package in the root folder and specify the following command to extract the install files from the tar file.

```
tar -zxvf <install_filename>
```

Replace <*install_filename*> with the actual name of the install file.

2 Change to the directory where you extracted the installer:

```
cd <directory_name>
```

3 Extract the appropriate `.tar.gz` file for your platform.

4 (Conditional) Specify the following command to enable FIPS:

```
./enablefips.sh on
```

NOTE: Do not restrict communication security settings to Federal Information Processing Standard (FIPS) encrypted algorithms unless you are certain that your environment requires that restriction. If you enable FIPS 140-2 mode, UNIX Agent Manager cannot communicate with Agents that are running in non-FIPS mode. For more information about FIPS and the other security level options, see Chapter 5, “Converting Agent from Non-FIPS to FIPS mode,” on page 31.

5 Specify the following command to install the UNIX Agent Manager in the new `UAM` folder:

```
./installserver.sh install
```

6 Specify and confirm a password for the UNIX Agent Manager server. The administrator user account can use this password.

7 Run the following script to create the UNIX Agent Manager database and set the administrator password before you run the `run.sh` script:

```
./runserver.sh
```

8 Run the following script to start the UNIX Agent Manager console:

```
./run.sh
```

9 Continue with the installation as prompted until the installation is complete.

Installing Security Agent for UNIX

This topic provides information about the various ways to install Security Agent for UNIX.

Remote Installation Using UNIX Agent Manager

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

- 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.

To remotely deploy the Agent components:

1 Launch UNIX Agent Manager.

2 Go to **File** > **Remote Deployment**.

3 Select **Add Host**, specify the host name of the computer on which you want to install the Agent and click **OK**.

4 Select the checkbox next to the added host, fill in all the details on the right panel, and click **Next**.

5 Specify the **User name** and **Password** of the target computer.

6 Select **Create a new configuration** in the **Prepare Agent Configuration** window and click **Next**.

NOTE: If you have already saved the configuration file from a previous installation or silent installation file, you can use the other options accordingly.

---

7 (Conditional) If you have already installed components on host(s) and want to use them, select **Add the selected components to the existing install** in the **Installation type**.

8 (Conditional) If you are installing the components on the host(s) newly, select **Create a new install with the selected components** in the **Installation type**. This will remove any components already installed on the host(s), including AppManager components.

9 Select the required components to install and click **Next**.

10 (Conditional) Go to the **Required Configuration** window, specify the **Port** as 2620 and select **Enable FIPS Security Restrictions**, and complete the installation.

NOTE: Do not restrict communication security settings to Federal Information Processing Standard (FIPS) encrypted algorithms unless you are certain that your environment requires that restriction. If you enable FIPS 140-2 mode, UNIX Agent Manager cannot communicate with Agents that are running in non-FIPS mode. For more information about FIPS and the other security level options, see Chapter 5, “Converting Agent from Non-FIPS to FIPS mode,” on page 31.

---

11 When prompted, specify `rclink`. `rclink` is the default option for restart method. For more information about restart methods, see "Restart Methods for the Security Agent for UNIX" on page 68.

12 (Conditional) If you are monitoring Secure Configuration Manager servers, go to the **Secure Configuration Manager Configuration** window and specify the following:

- **uvserv Port**: Enter 1622.
- **Hostname**: Specify the host name.
- **Port**: Enter 1627.
- **SCM Core Version**: Specify the version of Secure Configuration Manager server.

NOTE: To enable FIPS communication between the Agent and Secure Configuration Manager server, select the checkbox next to **Enable FIPS Security Restrictions**.

---

13 (Conditional) If you are monitoring Change Guardian servers, go to the **Change Guardian Configuration** window and specify the following:

- **CGU Component Startup Type**: Select `rc scripts`.
- **Hostname**: Specify the host name.
- **Port**: Enter 8094.
- **Username**: Enter the user name.
- **Password**: Enter the password.

NOTE: You can specify the other details and click **Next**.

---

14 (Conditional) If you are monitoring Sentinel servers, go to the **Sentinel Configuration** window and specify the following:

- **Sentinel Component Startup Type**: Select `rc scripts`.
- **Hostname**: Specify the host name.
- **Port**: Enter 1590.
- **Failover 1**: Specify the IP address of the first server.
- **Failover 2**: Specify the IP address of the second server.
- **SNMP Console Host Name**: Specify the IP address of the SNMP host.

NOTE: You can specify the other details and click **Next**.

---

15 Continue with the installation as prompted until the installation is complete.

16 (Conditional) If you are monitoring Oracle databases with Sentinel, provide the configuration information for the computer by clicking **Configure > Sentinel Options > Configure Oracle Endpoints**.

To add a host in UNIX Agent Manager, where the Agent is already installed:

1 Go to **Manage Hosts** > **Add Host**.

2 Enter the host name or IP address of the computer on which the Agent is already installed.

3 When prompted, enter the UNIX Agent Manager database account **Username** and **Password**.

4 Click **Add Host** button to add the host.

Local Installation

The following procedure guides you through logging on to the endpoints and locally installing the Agent computer.

To install an Agent on a local computer:

1. Log on to an Agent computer using an account with superuser privileges.
2. Download the package in the root folder and specify the following command to extract the install files from the tar file.

   ```
   tar -zxvf <install_filename>
   ```

   Replace *<install_filename>* with the actual name of the install file.
3. Change to the directory where you extracted the installer:

   ```
   cd <directory_name>
   ```
4. Specify the following command to start the install script:

   ```
   /bin/sh ./install.sh
   ```
5. (Conditional) If a compatible agent is already installed, enter **y** when you are prompted with the following text:

   ```
   A compatible agent is already installed on this machine in the directory '/
   usr'. Do you want to add or upgrade existing agents to it?
   ```
6. (Conditional) If you are installing a new agent, when prompted, enter **/usr** and proceed through the prompts.
7. (Conditional) To install the Agent in FIPS mode, enter **y** when you are prompted with the following text in the command prompt:

   ```
   Do you want to enable FIPS security restrictions for communication with this
   component? [n]
   ```

   The default value is **n**.
8. Proceed through the prompts.
9. Enter **y** if you want the Agent to monitor other NetIQ security products. Otherwise, enter **n**.
10. When prompted, specify `rclink`.

    `rclink` is the default option for restart method. For more information about restart methods, see "Restart Methods for the Security Agent for UNIX" on page 68.
11. (Conditional) If you are using Sentinel, when the installation completes, add the host using UNIX Agent Manager for deploying the Sentinel rules. For information about how to deploy rules, see "Activating Rule Sets" on page 45.
12. (Conditional) If you are monitoring Oracle databases with Sentinel, provide the configuration information for the computer by clicking **Configure**> **Sentinel Options** > **Configure Oracle Endpoints**.

The installation process finishes and the Agent starts. It might take a few minutes for all services to start after installation.

Silent Installation

The silent or unattended installation is useful if you need to install more than one Agent. Silent installation allows you to install the Agent without interactively running the installation script.

IMPORTANT: To perform silent installation, ensure that you have recorded the installation parameters during the interactive installation and then run the recorded file on other endpoints. 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`.

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

If you use the deployment wizard to perform local installation on one computer, you can create a silent installation file based on your requirement. A sample installation file, `SampleSilentInstallation.cfg`, is located in your Agent download package.

To perform a silent installation:

1. Download the installation files from the NetIQ Downloads website.
2. Download the package in the root folder and specify the following command to extract the install files from the tar file:

   ```
   tar -zxvf <install_filename>
   ```

   Replace <*install_filename*> with the actual name of the install file.
3. After you create the installation file, you can run silent installation on the endpoints from command line using the following command:

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

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

NOTE: If you are using the Agent with Sentinel, perform additional steps after the silent installation:

- Deploy the Sentinel rules using UNIX Agent Manager on the Agent computer. For information about how to deploy rules, see "Activating Rule Sets" on page 45.
- Configure Oracle database monitoring by clicking **Configure**> **Sentinel Options** > **Configure Oracle Endpoints**.

Following is the list of parameters that you can use during silent installation:

Parameter	Description
`FRESH_INSTALL`	Specifies whether you want to install or upgrade the Agent. Valid entries are `1` (install) and `0` (upgrade). The default value 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 value 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 value is `n`.

Parameter	Description
IQCONNECT_PORT	Specifies the port that the Agent uses to listen for communications from UNIX Agent Manager. The default value is 2620.
IQ_STARTUP	Specify restart method for the uagent process. For information about the options, see “Restart Methods for the Security Agent for UNIX” on page 68. Valid entries are rclink and inittab. The default option is rclink.
USE__COMMON	Specifies whether the Agent communicates with UNIX Agent Manager in FIPS mode. For more information about this option, see Chapter 5, “Converting Agent from Non-FIPS to FIPS mode,” on page 31. The default value is 0.
INSTALL_SENTINEL	Specifies whether the Agent works with Sentinel. Valid entries are y and n.
SENTINEL_ADDR=	Specifies the IP address of the primary Sentinel Agent Manager Server SSL.
SENTINEL_PORT	Specifies the port that the Agent will use to communicate with Sentinel. The default value is 1590.
SENTINEL_FAILOVER1_ADDR=	Specifies the IP address of the failover Sentinel that the Agent will attempt to contact if the primary Sentinel does not respond.
SENTINEL_FAILOVER1_PORT=	Specifies the port that the Agent will use to communicate with the first failover Sentinel. The default value is 1590.
SENTINEL_FAILOVER2_ADDR=	Specifies the IP address of the failover Sentinel server that the Agent will attempt to contact if the first failover Sentinel does not respond.
SENTINEL_FAILOVER2_PORT=	Specifies the port that the Agent will use to communicate with the second failover Sentinel server. The default value is 1590.
SENTINEL_PRIMARY_RETRY	Specifies how many seconds you want the Agent to wait before attempting to reconnect to a primary computer that does not respond.
SENTINEL_SNMP_TRAPS	Specifies the port that the Agent will monitor for SNMP notifications.
SENTINEL_LOW_DISK	Specifies the minimum disk space in bytes that are required to run the Agent. If the disk space falls below this limit, then the Agent will stop monitoring.
SENTINEL_STARTUP	Specifies restart method for the Agent. For information about the options, see “Restart Methods for the Security Agent for UNIX” on page 68. Valid entries are rclink and inittab. The default value is rclink.
INSTALL_SCM	Specifies whether the Agent works with Secure Configuration Manager. Valid entries are y and n.
SCM_CORE_ADDR	Specifies the IP address of the computer where you installed Secure Configuration Manager Core Services.
SCM_CORE_PORT	Specifies the port that the Agent will use to communicate with Secure Configuration Manager Core Services.

Parameter	Description
SCM_UVSERV_PORT	Specifies the port that the Agent will use to communicate with Secure Configuration Manager.
SCM_UVSERV_STARTUP	Specifies the restart method for the uvserv process. For information about the options, see "Restart Methods for the Security Agent for UNIX" on page 68. Valid entries are rclink, inetd, and inittab. The default value is rclink.
USE_FIPS_SCM	Specifies whether the Agent communicates with Secure Configuration Manager in FIPS mode. Use this option if your environment requires FIPS. For more information, see "Restart Methods for the Security Agent for UNIX" on page 68. Valid entries are 0, communication is not restricted, and 1, communication is restricted. The default value is 0.
INSTALL_CGU	Specifies whether the Agent works with Change Guardian. Valid entries are y and n.
IQRM_ADDR	Specifies the IP address of the computer where you installed the Change Guardian Policy Repository.
IQRM_PORT	Specifies the port that the Agent will use to communicate with the Change Guardian Policy Repository. The default value is 8094.
IQRM_USER	Specifies the account that the Agent uses when accessing the Change Guardian Policy Repository.
IQRM_PASS	Specifies the password for the account that the Agent uses when accessing the Change Guardian Policy Repository.
IQCONFIG_RECONNECT	Specifies how often, in minutes, the Agent checks for new information in the Change Guardian Policy Repository. For example, 2.
CGU_STARTUP	Specifies restart method for the detected process. For information about the options, see "Restart Methods for the Security Agent for UNIX" on page 68. Valid entries are rclink and inittab. The default value is rclink.
MANAGE_AUDIT_LOGS	Specifies whether the Agent reduces the size and removes old audit logs. Valid entries are y and n.
AUDIT_LOG_SIZE	Specifies the maximum size, in bytes, that the Agent allows an audit log to reach before starting a new log.
AUDIT_LOG_RETENTION	Specifies the number of audit logs that the Agent keeps. Once this number of audit logs exists, the Agent will delete old logs when making new ones.
KEEP_OLD_AGENT_DIR	Specifies whether to keep the previous installation directory when you are upgrading the Agent. Valid entries are y and n.
OLD_INSTALL_DIR_MOVED	Specifies the directory where you want the installation program to move to the previous installation directory.

4 Managing Users Using UNIX Agent Manager

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

Example: You can create a permission set that grants access to all products' functionality. You can then assign this permission set to all the computers. When you grant a new user access to a console, simply assign the user to that particular permission set to grant them access to the applicable features and computers.

To assign permissions, log on to UNIX Agent Manager console as an administrator, click **Access Control** > **Admin Console**. Add the users that need access to that UNIX Agent Manager server, then assign the appropriate permissions that are listed in the **Permissions** tab.

- "Configuring UNIX Agent Manager Server to Use LDAP or Microsoft Active Directory Credentials" on page 29
- "Using SSL with LDAP or Active Directory Server for Communicating with UNIX Agent Manager" on page 30

Configuring UNIX Agent Manager Server to Use 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 on to the UNIX Agent Manager server. This functionality is not available if UNIX Agent Manager is installed in FIPS mode.

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

1. Ensure that you have the following information:
   - The domain and computer address, such as `ldap://<ldap_ip_address>:389`, of the LDAP or Active Directory server
   - Location of user entries in the structure of LDAP or Active Directory server
   - Attribute that identifies the login name for each user
   - An account that the UNIX Agent Manager server can use to access the LDAP or Active Directory server
2. Log on to UNIX Agent Manager as an administrator, and open the **Manage Server** window.
3. Click **LDAP** and then click **Add** button.
4. Enter the name of the domain that contains the LDAP or Active Directory server.

NOTE: Users must enter this domain name when they log on to UNIX Agent Manager.

5. Select the domain and provide information as requested on the window using the following guidelines:
   - In **Server Address**, enter the LDAP or Active Directory server computer name and port. For example, `ldap://<ldap_ip_address>:389`
   - In **User's Parent DN**, enter the path to the node that contains the user name. For example, `ou=AMAdmins,dc=netiq,dn=com`
   - In **Username**, enter the attribute you want UNIX Agent Manager to use to identify the user. It will be used as a consistent identifier even if the user name changes. The default and only attribute supported by UNIX Agent Manager 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 **Refresh Users**.

Using SSL with LDAP or Active Directory Server for Communicating with UNIX Agent Manager

The UNIX Agent Manager server can communicate with the LDAP or Active Directory server using Secure Sockets Layer (SSL). If you choose UNIX Agent Manager server to 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 a `.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 process:

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

NOTE: For more information about LDAP authentication, see Logging in by Using LDAP User Credentials in *The NetIQ Sentinel Administration Guide*.

5 Converting Agent from Non-FIPS to FIPS mode

This chapter provides the procedure to convert the Agent to FIPS mode when it is already installed in non-FIPS mode.

NOTE: Once you have converted the Agent to FIPS mode, you cannot revert the Agent to non-FIPS mode.

To convert an existing Agent in non-FIPS mode to FIPS mode:

1. Open the Agent configuration file `/etc/vigilent.conf` in edit mode.
2. Search for the parameter *useFipsMode* and set the value of this parameter to **1**.
3. Restart the Agent and check if the Agent is running in FIPS mode.

   NOTE: For more information on how to restart the Agent see, “Restart Methods for the Security Agent for UNIX” on page 68.

   ---

4. Ensure that the `VigilEntAgent_2620.log` file (located in `cmnagent/log`) contains the following entry: `INFO [Date_Timestamp, PID:<pid_number> [vosSSLCodec] FIPS mode enable succeeded`

6 Configuring Agent for Secure Configuration Manager

Secure Configuration Manager manages all agents such as Windows Agents and iSeries Agents that monitor UNIX computers in the same way as it does for any other kind of Agent, with no special configuration necessary. However, if you are monitoring Oracle database, you must ensure that the endpoints are configured correctly. To configure Secure Configuration Manager to monitor Oracle, you must first install Agent on the computer running on Oracle, then you can add one or more Oracle endpoints to the new Agent.

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

To add Oracle endpoints to Agent, use the following steps:

1. Install the Agent on the computer running on Oracle.
2. Navigate to **NetIQ Secure Configuration Manager** > **IT Assets** >**Agents** > **OS** > **Unix**.
3. In the content pane, select the Agent to which you want to add the endpoint.
4. In the **Actions** menu, click **Add Endpoint**.
5. Select the Agent you want the endpoint to monitor and click **Next**.
6. In the **Name** field, type a name for the endpoint.
7. In the **Endpoint Type** field, select **Oracle**.
8. Specify the required information in the following fields.
   - **Oracle Instance ID:** Name of the Oracle instance
   - **User Name:** User account used to access the Oracle database. If your Oracle environment requires the `name@sid` format, use that format here. This account must have access to read tables and views. The specific requirements for access depend on which checks you run. You must assign adequate permission for the checks you use to access the information you need.
   - **Password**: Password for the user account used to access the Oracle database.
9. (Optional) If you want to add more information about the endpoint, specify the following optional fields.
   - **Contact Email**: Email address of the contact person.
   - **Contact Name**: Name of the designated contact person.
   - **Importance**: Criticality level of the endpoint.
   - **Location**: Geographical location of the computer hardware.
   - **Major Version**: Version of Oracle the endpoint is running.
10. (Conditional) If you want to add the endpoint to a group, complete the following steps:
    - **10a** Click **Add Endpoint to a Group**.
    - **10b** Select an existing group to which you want to add the endpoint, or click **Create** to create a new group.
    - **10c** Click **Finish** to return to the Define Endpoint window.

11 (Conditional) If you are adding more than one endpoint, click **Add Endpoint**. Repeat Step 5 through Step 9 for each endpoint that you want to add.

12 Click **Finish**.

For more information about see, Secure Configuration Manager documentation.

NOTE: For information about Lightweight UNIX solution see, Using the Lightweight UNIX Solution in Secure Configuration Manager User guide.

---

7 Configuring Agent for Change Guardian

Change Guardian requires you to enable the auditing system of your operating system. If you have already enabled auditing and Change Guardian is functioning successfully, your operating system is correctly configured. However, if you are not receiving events, use the information in this chapter to configure auditing for your operating system.

NOTE: You must enable auditing to configure the Agent with Change Guardian.

Configuring a UNIX Auditing Subsystem

This section provides information about auditing on UNIX computers.

Configuring the AIX Audit Subsystem

The auditing subsystem on AIX computers stores files in the `/etc/security/audit` folder. Enable the audit streaming. However, streaming all events might consume too much memory or processor time, so switch on only the minimum required auditing.

The minimum auditing activity Change Guardian requires the following:

1. Add the following line to the `/etc/security/audit/config` and `/etc/security/audit/streamcmds` files:

   ```
   /usr/sbin/auditstream | /usr/sbin/auditpr -t 0 -r -v -helRtcrpPTh >> /audit/stream.out&
   ```

2. Ensure that the `/etc/security/audit/config` file includes the following lines:

   ```
   start
        binmode = off
        streammode = on
   bin:
        trail = /audit/trail
        bin1 = /audit/bin1
        bin2 = /audit/bin2
        binsize = 10240
     cmds = /etc/security/audit/bincmds
   stream:
     cmds = /etc/security/audit/streamcmds
   ```

```
classes:

     general =
USER_SU,PASSWORD_Change,FILE_Unlink,FILE_Link,FILE_Rename,FS_Chdir,FS_Fchdir,F
S_Chroot,PORT_Locked,PORT_Change,FS_Mkdir,FS_Rmdir,FILE_Symlink,USER_Exit,PROC
_Create,PROC_Delete,FILE_Fchmod,FS_Rmdir,GROUP_User,GROUP_Adms,GROUP_Change,GR
OUP_Create,GROUP_Remove,USER_Remove,USER_Create,USER_Chpass,USER_Change,FS_Mou
nt,FS_Umount,FILE_Unlinkat,FILE_Symlinkat

     Kernel =
PROC_Create,PROC_Delete,PROC_Execute,PROC_RealUID,PROC_AuditID,PROC_RealGID,PR
OC_Environ,PROC_SetSignal,PROC_Limits,PROC_SetPri,PROC_Setpri,PROC_Privilege,P
ROC_Settimer,PROC_LPExecute,PROC_Adjtime,PROC_Kill

     files =
FILE_Open,FILE_Read,FILE_Write,FILE_Close,FILE_Link,FILE_Unlink,FILE_Rename,FI
LE_Owner,FILE_Mode,FILE_Acl,FILE_Privilege,DEV_Create,FILE_Dupfd,FILE_Chmod,FI
LE_Chown,FILE_Utimes,FILE_Truncate,FILE_Mknod,FILE_Symlink,FILE_Unlinkat,FILE_
Fchownat,FILE_Linkat,FILE_Fchown,FILE_Symlinkat,FILE_Openxat,FILE_Mknodat,FILE
_Renameat,FILE_Fchownat,FILE_Fchmod,FILE_Fchown,FILE_Fchmodat


     cron =
AT_JobAdd,AT_JobRemove,CRON_JobAdd,CRON_JobRemove,CRON_Start,CRON_Finish

users:

     root = general,kernel,files,cron

     default = general,kernel,files,cron

role:

     /usr/sbin/auditstream | /usr/sbin/auditpr -t 0 -r -v -helRtcrpPTh >> /usr/
audit/stream.out&
```

3 Ensure that the `/etc/security/audit/events` file contains the following:

- FS_Mount
- FILE_Unlinkat
- CRON_Finish
- FILE_Linkat
- CRON_JobRemove
- PROC_Kill
- PROC_Execute
- FILE_Unlink
- FILE_Rename
- FILE_Fchown
- FILE_Owner
- FILE_Close
- USER_Chpass
- FILE_Symlinkat
- USER_Change
- FILE_Symlink
- PROC_LPExecute

- FILE_Open
- FILE_Mknodat
- FILE_Dupfd
- FILE_Chmod
- FILE_Renameat
- USER_Create
- GROUP_Create
- FS_Chdir
- FS_Umount
- FILE_Chown
- FILE_Fchownat
- GROUP_Change
- PROC_Create
- USER_Remove
- FILE_Fchmod
- PROC_Adjtime
- CRON_JobAdd
- FILE_Utimes
- PROC_Delete
- FILE_Openxat
- GROUP_Remove
- FILE_Fchmodat
- FILE_Mode
- PROC_Settimer
- FILE_Mknod
- CRON_Start
- FILE_Link

NOTE: If your attempt to set up auditing on your AIX computer is not successful, ensure that you remove all files in the `/etc/security/audit` directory except the `trail`, `stream.out`, and the `bin` directory.

Configuring the HP-UX Audit Subsystem

The auditing subsystem on HP computers stores files in the `/etc/rc.config.d` directory. You must process audit trail events. Ensure that the `/etc/rc.config.d/auditing` file matches the following lines:

```
AUDITING=1

PRI_AUDFILE=/.secure/etc/audfile1

PRI_SWITCH=1000

SEC_AUDFILE=/.secure/etc/audfile2
```

```
SEC_SWITCH=1000

AUDEVENT_ARGS1=" -P -F   -e admin -s exit -s kill -s vfsmount -s rename -s unlink -
s creat -s symlink -s fchown -s execv -s stime -s link -s settimeofday -s mount -s
clock_settime -s fchmod -s lchown -s umount2 -s chmod -s execve -s chown -s open -
s umount -s fork -s mknod -s vfork -s chdir -s adjtime -s mkdir -s rmdir  "

AUDEVENT_ARGS2=" "

AUDEVENT_ARGS3=" "

AUDEVENT_ARGS4=" "

AUDOMON_ARGS=" -p 20 -t 1 -w 90"
```

Configuring the Solaris Auditing Subsystem

Solaris 10 operating system has different auditing subsystems than Solaris 11.

On computers running Solaris 10, perform the following steps:

1. Ensure that the Basic Security Module restarts after reboot by running `./bsmconv` from the `/etc/security` folder.
2. Ensure that the `/etc/security/audit_control` file contains the following lines:

   ```
   flags: ua,fm,cl,pc,fw,fr,ad,as,fc,ps,fd,nf

   naflags: fm,cl,pc,fw,fr,as,ad,fc,ps,fd,nf

   minfree:20

   dir:/var/audit
   ```

For Solaris 11, set the auditing flags by running the following commands:

```
auditconfig -setflags pm,ps,ua,as,fd,fc,fm,fw,fr

auditconfig -setnaflags pm,ps,ua,as,fd,fc,fm,fw,fr
```

Configuring a Linux Auditing Subsystem

Auditing subsystems on SUSE, RHEL, and RHEL variants are very similar. There are some differences in configuration based on operating system and on architecture.

NOTE: For RHEL and SUSE platforms, configure the audit daemon in the `/etc/audit/auditd.conf` file.

Perform the following steps to configure auditing on a Linux computer:

1. (Conditional) For RHEL, run the following command to ensure that the `auditd` service is enabled:

   ```
   # chkconfig auditd on
   ```
2. (Conditional) For SUSE, perform the following steps:
   1. Check if the process is running by entering the command:.

      ```
      # ps -ef | grep -i audit
      ```

In the command output, if the audit process is running in disabled mode, to start the process in enabled mode, enter the command `# /sbin/auditd -s enable`.

2. Ensure that the PID in the command output matches with the PID of the process enabled, by running the following command:

   ```
   # auditctl -e 1
   ```

NOTE: After you upgrade from Security Agent for UNIX 7.4 to 7.5 version, remove the system calls from the `/etc/audit/audit.rules` file that might have been added for Security Agent for UNIX 7.4.

For agents that are running on Linux platforms, additional audit configuration is performed dynamically as Change Guardian policies are enabled and disabled.

8 Configuring Agent for Sentinel

This chapter provides information about configuring agents to send events to Sentinel. Ensure that you have configured your agents to communicate with Sentinel.

For more information about rules, see Chapter 9, “Understanding Security Rules for Sentinel,” on page 43.

Configuring the Agent with Oracle

If you use Sentinel to monitor Oracle on UNIX or Linux, you must use UNIX Agent Manager to register the Oracle database and specify an account with access to read the **table** and **views**.

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 that you want to monitor.
2. Go to **Configure** > **Sentinel Options**.
3. Select the host with the Oracle database you want to monitor.
4. Click **Manage Oracle Endpoints** > **Add**.
5. Specify the following fields under **Instance Configuration**:
   a. **User Name**: Enter the Oracle user name that has Database Administrator (DBA) permissions.
   b. **Password**: Enter the password of DBA user.
6. Click **Register Endpoints**.
7. Activate the Oracle rule set. For more information about activating rule sets, see “Deploying Rule Sets” on page 41.

Deploying Rule Sets

Complete the following steps to activate the rule set delivered with the latest version of UNIX Agent Manager on your Agent computers. These rules that you configure perform event detection and alerting to send events that are filtered based on rules deployed to Sentinel.

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.
4. After you made changes to the rule set, save a copy by clicking **File** > **Save/Save All** and close the Save window.
5. In the **Available Hosts** list, select the Agent computers on which you want to deploy the rule set.
6. Click **File** > **To Select Hosts**.

7 Click **Select** to deploy the rule set. It might 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 **Sentinel** column shows **green cells** for all agents with an active rule set.

Enabling Process Accounting

You can enhance security event reporting in Sentinel by enabling process accounting. However, enabling process accounting substantially increases the activity on the monitored computer and also changes the base computer configuration, which might not be acceptable for your environment. Enabling process accounting is optional. Do not enable these modules if syslog reports the events you want to monitor.

For more information, see the respective Collector documentation on Plugins documentation page.

Configuring Your Auditing System for Groups

To configure and enable auditing on your computers for **Groups**, ensure that your operating system auditing is configured to report the required information.

- To monitor AIX, you must process audit events and check if the auditing subsystem is configured and activated.
- To monitor HP, you must process the HP-UX audit trail events.
- To monitor Linux, you must process the Linux audit trail events.
- To enable auditing on computers using Solaris operating systems, classes of events must be selected for auditing.
- To monitor Oracle, also register the endpoint in UNIX Agent Manager. This rule group contains rules that process Oracle audit events.

For more information, see the respective Collector documentation on Plugins documentation page.

9 Understanding Security Rules for Sentinel

This chapter provides an overview of 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**.

Understanding Security Agent for UNIX Rules

You can protect your information assets and ensure that uniform security by applying Agent rule sets. By working in conjunction with the event detection and alerting process, 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 processes
- Running specific sensitive commands
- Running sensitive commands as a non-root user
- Creating, modifying, or deleting specific files

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

Understanding Rule Sets

Rule sets are collections of rules you want to enforce on a specific Agent computer or a group of 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 servers such as, Apache web servers or Oracle database servers. You can enforce unique rule sets on each 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.

Selecting a Rule Set to Edit

Before you start working with a rule set, determine which 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 and click **Create Rule Set**. If you modify the default rule set, save the new rule set with a unique name.
- Open a saved rule set if you have already begun to edit a rule set. 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 on selecting a rule set, see “Understanding Rule Sets” on page 44

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 “Understanding Event Sources” on page 46.
- Rule groups provide editable properties at the group level, and contain individual rules. For more information, see “Understanding Rule Groups” on page 47.
- Expanding a rule group allows you to view and edit the rules associated with its common event source. For more information, see “Understanding Rules” on page 47

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

Editing Rule Set 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 a rule or rule group, perform the following steps:

1. Right-click the rule in the tree pane.

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.

Activating Rule Sets

Deploying a rule set to an Agent computer replaces the previous rule set. The event detection and alerting processes begin processing and initializing the new rule set immediately. However, it might take up to 30 seconds for the new rule set to take effect. Modifications to items in the `filesystem` rule group might cause the event detection and alerting process might take longer to initialize, because of the time it takes to create initial snapshots of the `filesystem` objects.

To deploy rule sets to Agent computers:

1 Start the UNIX Agent Manager.

2 Click **File** > **Rules Manager**.

3 Click **Manage Rule Sets** > **Create Rule Set**, and then enter a name for rule set.

4 (Conditional) If you want to make changes to the default rule set displayed in the Rules Manager, customize the rule set as needed until the rule set is correctly configured for your environment.

5 Close the Rule Editor.

6 Click **Back** to return to the main Rules Management window.

7 In the Available Hosts list, select the Agent computers on which you want to use the rule set.

8 Click **To Selected Hosts** to deploy the rule set. The `detectd` process begins processing and initializing the new rule set immediately. However, it might take up to 30 seconds for the new rule set to take effect.

9 Verify that the rule set is active on the Agent computers. The **Sentinel** column shows green cells for all agents with an active rule set.

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 process terminates.
- Rules that trigger when a log file decreases in size.
- Rules that trigger when certain commands are run by root.
- Rules that trigger when certain commands are run by users other than root.
- Rules that trigger when certain files are changed or created.
- Rules that trigger when anything in the system changes. For example: Login, logout, auditing.

To start the wizard, click **Edit Rule Set** in **Rules Management** screen, then click **Wizard** > **Rule Wizard**, and continue with the configuration as prompted.

Using the Rule Wizard to Create Rules

The Rule wizard helps you to quickly create the different types of rules.

To use the Rule Wizard to create rules:

1. Click **Wizard** > **Rule Wizard** to start the Rule wizard.
2. In the select Rule Type window, select the appropriate rule type, and then click **Next**. For more information about rule type see, “Understanding Rules” on page 47.
3. In the Rule Description window, provide a name for the rule, and then click **Next**.
4. In 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 process to monitor all files with a certain name. Selecting **Paths** causes the event detection and alerting process to monitor a specific file.
6. In the Name of File window, specify the name of the object you want to monitor and click **Next**. The name depends on the selected rule type, which might be a process 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 about rules and actions see, “Understanding Rules” on page 47
8. Review the information provided about the rule group associated with your rule, and then click **Next**.
9. Specify the required information in 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 provided descriptions and, if necessary, modify the parameters. If you are unsure about the correct values, retain the current values.
10. Click **Finish**.

Understanding Event Sources

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

- Operating system
- Processes
- Server
- Application

Typically, event sources extract the required information by parsing and filtering log entries. When 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 process.

When an event source detects an event and assigns output parameter values, the event detection and alerting process uses the values to trigger the appropriate rule response in the associated rule group.

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. Duplicate the monitoring, parsing, and output parameter generation between instances of the event source. Specify the event source of a rule group by editing the properties of its corresponding rule group.

To add an event source to a rule set, right-click **Rule Set** > **Add Event Source** in the Edit Rules window.

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:

- Attributes
  - Name
  - Description
- Event source
  - Event source
  - Event source Configuration Parameters
- Advanced
  - Nice value
  - Delay (seconds)
  - Debug Level

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

To create a new rule group, right-click **Rule Set** in the Edit Rules window.

Understanding Rules

Rules contain all of the information the event detection and alerting process 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:

Properties	For more information, see
Actions	“Understanding Actions” on page 48
Initialization code	“Understanding Initialization Code” on page 49
Main code	“Understanding Main Code” on page 50
Conditionals (And and Or objects)	“Understanding Conditionals and Comparisons” on page 49

Properties	For more information, see
Comparisons	“Understanding Conditionals and Comparisons” on page 49
Time conditions	“Understanding Time Conditions” on page 50
Templates	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.

Understanding Actions

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. Specify these fields with the appropriate information. Separate multiple e-mail addresses with a comma. You must have Agent configured correctly on the Agent computer to send e-mail.
- **SNMP**: 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.
- **Sentinel Event**: Specifies the NetIQ classification attribute used to classify events for Sentinel.

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 rule properties, right-click the rule in the Edit Rules window.

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

Creating New Rules and Actions

Creating new rules can be a time consuming task. Before creating new rules, ensure that you have investigated that 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.

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 that are not previously configured. If the rule configures itself through querying the operating system or process, the rule requires initialization code. Rule containing initialization code displays Init Code as a child element in the tree pane.

Understanding Conditionals and Comparisons

You must declare conditionals and comparisons to ensure that you trigger actions only when necessary. Conditionals and comparisons help you filter event source output parameters.

To trigger an action when both comparisons are met, 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 might have numerous child elements. Rules that do not have conditional or comparison statements must have main code to trigger. For more information about the main code see, “Understanding Main Code” on page 50.

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 process evaluates the statement as true.

To edit comparisons or conditionals, right-click the rule you want to modify. To associate comparisons with a conditional, right-click the conditional, and then click **Add Comparison**. Comparisons are labeled with the output parameter name, equation, and value describing the comparison.

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

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.

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, perform the following steps.

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**.

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 that 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**.

Deleting Time Conditions

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

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

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. Rules that contain main code display the Code element in the rule.

Viewing and Editing Main Code

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

UNIX Agent Manager also allows you to edit the existing main code. Before editing code that functions correctly, ensure that you take a backup of the rule set. Perform the following procedure to edit your 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 about activating rule set see, “Activating Rule Sets” on page 45.

Adding New Main Code

UNIX Agent Manager allows you to add main code to a rule. Before adding main code, ensure that 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 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 in the UNIX Agent Manager computer and activate the modified rule set on remote Agent computers. For more information, see “Activating Rule Sets” on page 45.

Deleting Main Code

Before deleting main code, ensure that you no longer need the code to make the rule work. Perform the following procedure 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**.

Customizing the Rules Management User Interface

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

Deciding Whether to Use Tabbed Layouts

Tabbed layouts allow you to select how you want to view configuration information in the content area. The tabbed layout provides information grouped into specific categories, which is easy to read. You can navigate to other configuration categories by clicking the corresponding tab.

The non-tabbed layout option displays 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.

Deciding Whether to Use Parameter Aliases

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

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

When you configure rules using the descriptive aliases instead of the parameter name, the 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.

Deciding Whether to Use Hide Node Name Underscores

UNIX Agent Manager uses hide node name underscores to hide underscores in rule set, rule group, and parameters.

Deciding Whether to Use Hide Node Titles

UNIX Agent Manager uses hide node title to hide rule set title, rule title, group title from the left panel of the **Edit Rules** window.

Restricting Access to Rule Sets

The Agent provides variables that allow you to customize the access to rule sets. By default, the variables and associated parameters are specified in the `vsaunix.cfg` file. Some environments might benefit from limiting access to the rule sets to improve security or performance. The following table describes the variables.

Commands	Description
DETECTD_OPS	This command 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"`
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"`

Sample Rule Groups

This section lists a few examples about how you can create rule group for custom application.

The default installation creates a rule set that supports limited number of applications. The rule sets can be used as templates to create custom rule groups for new applications. The following example procedure provides the steps to create a Rule Group for Stash or BitBucket, which is used as a source code repository.

1. Click **Rules Manager**.

   The **Rules Management** window is displayed.

2. Click **Manage Rule Sets** > **Create Rule Set**.

3 Enter the name of the rule set and click **OK**.

The Rule set will be populated with default Event Sources and Groups.

4 To create a new rule group, in **Edit Rules** panel, right-click **Rule sets** and select one of the following options based on your requirement:

- **Add Event Source**: Event Sources are programmable entities and used by the rule group to get event stream. Event Sources pass the events to rule groups by setting output parameters.
- **Add Real-time Group**: Rule groups in the default rule set are real-time and contain information about rules. The rules are grouped based on the source of events.
- **Add Scheduled Group**: Rule groups created based on the schedule at which you want the Agent to monitor the systems.

5 Select the **Add event source** to create a custom event source for Stash or BitBucket.

The following are the tabs in the **Add Event Source** window:

- **Configuration**: Set as per the variable that is used for the log location.
- **Output**: Set by the event code and read by the rules.
- **Notifications**: SNMP notification that includes a configurable subset of the output parameters.
- **Sentinel Event**: Maps the output variable.
- **Attributes**: Name and description of the event source.
- **Initialization**: Contains the Perl code that is evaluated on startup. You can initialize variables, instantiate objects, and open file for reading the log files.

  Example of Initialization code: You can modify this code based on your requirement.

```
@logfiles = _globList(@{$logfilesOsTable{$^O}});
if($#logfiles &lt; 0)
{
 sleep(30);
 es_exit(0);
}
$#fileBfrs = -1;
foreach my $logfile (@logfiles)
{
my $fileBfr = PS_FileBuffer-&gt;new($logfile, 0, 1, $main::__group_name);
push(@fileBfrs, $fileBfr);
}
```

- **Event Code**: Contains the Perl code that is repeatedly evaluated to get new events. You can set the output parameter variables from event information.

  Example of Event code: You can modify this code based on your requirement.

```
($record, $nbrBytes, $utc_timestamp, $year,
$monthAbbrev, $monthNbr,
$day_of_month, $hour, $minute, $second, $host, $source,
$pid, $message, $facility, $severity)
```

```
= _getNextLogRecord(\&amp;_parseSyslogEvent, undef,
@fileBfrs);
```

6. (Conditional) If you selected **Add Real-time Group**, specify the following:
   - **Attributes**: Specify the name and description of the group.
   - **Event Source**: Configure the event source and browse to provide the log file location.
   - **Advanced**: Specify the following:

     Nice value: Nice value scale goes from -20 to 19. The lower the number the more priority any task gets. If the value is high the task will be set to the lowest priority and the CPU processes it whenever possible. The default nice value is zero.

     Delay: The delay value is the polling interval, or the interval in which the rule group checks for new events.

     Debug level: The debug level is used to increase the amount of information logged to error logs.
7. (Conditional) If you selected **Add Scheduled Group**, specify the following:
   - **Attributes**: Specify name, description, and schedule time of the group.
   - Specify **Nice value** in **Advanced** tab and click **OK**.
8. Go to the new rule group that you created, right-click and select **Edit Rules** > **Turn on Rule(s)**.
9. Save the configuration, and navigate to **Rules Management Window** > **Apply Rule Set**.
10. Select the host on which you want to deploy rule set, and click **To Selected Hosts**.

    The rule set will be successfully deployed on the host.

The following table provides information about the perl modules that are imported in the event source code and namespace with the exception of the default modules:

Perl modules	Description
`PS_Default, PS_Helpers, PS_FileBuffer, PS_FifoBuffer, PS_DOM_XML_Parser`	Default perl modules.
`PS_Pacct`	Used by the pacct event source.
`PS_Filesystem`	Used by the filesystem event source.
`PS_Lsof`	Used by the network event source earlier.
`PS_VigilEntAgent`	Used by the network event source.
`PS_BsmDirect`	Used by the bsm event source.
`PS_AIXAudit`	Used the AIX_Audit event source.
`PS_HPAudit`	Used by the HP_Audit event source.
`PS_Wtmp`	Used by the wtmp event source
`PS_OracleAudit`	Used by the Oracle_Audit event source.
`PS_FileBuffer`	• `_parseEventRegEx`: Takes a regular expression with sub-expressions and returns an array of substrings that match the sub-expressions. • `_parseSyslogEvent`: Parses syslog records. • `_parseSulogEvent`: parses sulog records.

10 Upgrading Security Agent for UNIX

This chapter provides information about upgrading the Agent.

Saving Agent Information to File

The UNIX Agent Manager server stores information about all the agents you monitor. However, storing the information to a separate file can be useful for backups or for copying the server to another computer.

NOTE: To store your Agent list and configuration information in a file outside the UNIX Agent Manager server, click **Manage Hosts** > **Export/Import Host Lists** in UNIX Agent Manager 7.2 or later.

If you are upgrading from UNIX Agent Manager 7.4 to 7.5 or later, you should save your configuration information before you upgrade so that you can import it after you upgrade.

To export the agent information from UNIX Agent Manager, perform the following steps:

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

   All the host information is exported from UNIX Agent Manager.

Upgrading UNIX Agent Manager 7.4 to 7.5 on Linux

IMPORTANT: UNIX Agent Manager on Linux does not support upgrading UNIX Agent Manager 7.4 to 7.5 version.

Prerequisite: UNIX Agent Manager on Linux 7.4 with agents installed and configured.

Perform the following procedure to migrate from UNIX Agent Manager 7.4 to 7.5 version:

1. Close all UNIX Agent Manager 7.4 applications.
2. Uninstall UNIX Agent Manager 7.4 on target host by running the `./installserver.sh remove` command.

NOTE: Do not delete the UNIX Agent Manager database folder. Retain it for migration to 7.5 version.

3 Go to UNIX Agent Manager 7.5 folder and install UNIX Agent Manager Linux 7.5 by running `./installserver.sh install` command.

4 Import the UNIX Agent Manager database folder `<UAM Directory>/UAM/UAMDB` from 7.4 version instead of setting up a new database.

NOTE: UNIX Agent Manager does not prompt for creation of database if UNIX Agent Manager database folder already exists in current directory.

5 Start UNIX Agent Manager 7.5 by running the `./run.sh` command.

6 Log in as admin user configured during the UNIX Agent Manager Linux 7.4 installation.

UNIX Agent Manager 7.5 launches successfully with UNIX Agent Manager 7.4 pre-configured agents.

Upgrading UNIX Agent Manager 7.4 to 7.5 on Microsoft Windows

Perform this procedure to upgrade UNIX Agent Manager 7.4 to 7.5 on Microsoft Windows.

1 Download the UNIX Agent Manager 7.5 installer from NetIQ Downloads website.

2 Run the UNIX Agent Manager 7.5 installer on a different computer.

NOTE: Do not run the UNIX Agent Manager 7.5 installer on the same computer where UNIX Agent Manager 7.4 is installed. If you run the installation on the same computer as UNIX Agent Manager 7.4, the communication between UNIX Agent Manager 7.5 and existing 7.4 agents will be lost.

3 Import the UNIX Agent Manager 7.4 database to UNIX Agent Manager 7.5 using the **Import Host** option.

IMPORTANT: You can also export the host list from UNIX Agent Manager 7.4 and import the host list to UNIX Agent Manager 7.5. You need to retain the password of the UNIX Agent Manager 7.4 version when you install UNIX Agent Manager 7.5.

UNIX Agent Manager 7.5 will launch successfully with UNIX Agent Manager 7.4 pre-configured agents.

Upgrading Agent Using UNIX Agent Manager

UNIX Agent Manager provides a utility to upgrade existing agents.

To upgrade agents using UNIX Agent Manager:

1 Go to **File** > **Remote Deployment**, select **Add Host** and enter the host name or IP address of the computer and then click **OK**.

2 Select the checkbox next to the host name or IP address listed in the **Hosts** list.

3 Provide the target computer details, and then click **Next**.

4 (Conditional) If you have a previously saved configuration, select **Load a saved configuration from a previous installation**, and select the configuration file.

5 (Conditional) If you want to create a new configuration, perform the following:

1. Go to **File** > **Remote Deployment** and select **Add Host**.
2. In the **Prepare Agent Configuration** window, select **Create a new configuration** and click **Next**.
3. In the **Installation Type** window, select **Add the selected components to the existing install**, and then click **Next**.

   NOTE: For a successful upgrade, select all the components which are already running on the agent.

4. In the **Configuration Summary** window, click **Save this configuration for later use**.
5. Provide the name of the file and continue with the configurations as prompted.

   The install configuration file will be created.

6 Click **Next** and continue with the installation.

Applying Patches

NetIQ provides patches to the 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 UNIX Agent Manager** on the Start menu. To update UNIX Agent Manager on Linux, run the `update.sh` command.

To apply a patch to the Agent computer using the UNIX Agent Manager, perform the following steps:

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**.

6 Click **Back** to close the Patch Manager.

To apply a patch to the Agent computer manually, perform the following steps:

1 Copy the patch file to the `/usr/netiq/bin` directory.

2 Unzip the files and save them in the same directory.

3 Search the `wcPatch` file and run it.

4 Continue with the installation as prompted until the installation is complete.

5 Update and verify the `detectd` and `vigilentAgent` services.

11 Uninstalling Security Agent for UNIX

This chapter provides information about uninstalling the Agent and Agent components.

Uninstalling Security Agent for UNIX

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 that are for specific NetIQ security products.

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

When you run uninstall script for selected components, the dependent component will also be uninstalled.

Following are the scenarios:

- If you uninstall Sentinel agent, Change Guardian agent is also uninstalled.
- If you uninstall Change Guardian agent, Sentinel agent is also uninstalled.
- Secure Configuration Manager agent does not have any dependency on the other components

To uninstall the Agent locally, go to the installation directory, then run the following command:

```
./uninstall.sh
```

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

Uninstalling UNIX Agent Manager

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

To uninstall the UNIX Agent Manager on a Linux computer, go to the UNIX Agent Manager installation directory and run the following command:

```
installserver.sh remove
```

When you have completed the uninstall program, you can remove the UNIX Agent Manager directory by running `rm -rf UAM`.

Post-Uninstallation Tasks

Perform the following tasks to check if the uninstallation is successful:

- Check if all the components are uninstalled.

  Run `vi` command on `/etc/vsaunix.cfg` configuration file to check if the `unix agent fpr Cg` parameter is `n`.
- Verify the `/usr/sbin` folder to ensure that none of the services are running.
- Check if the Agent is uninstalled successfully.
- Check if the folder structure is deleted.

From UNIX Agent Manager, you can check if the uninstall is successful by navigating to **Manage Hosts**. The host or asset that is uninstalled should not be listed in the list of hosts.

12 Troubleshooting

This section helps you to troubleshoot issues that might occur when using Security Agent for UNIX.

Unable to Connect to Port

Issue: The Agent is not able to connect to the port.

Workaround: Run the following command to check whether the port 8094 is running:

```
netstat -an | grep 8094
```

Unable to Run the Services

Issue: The services are not running.

Workaround: Run the following commands to check whether the **detectd**, **vigilent**, **auditd** services are running.

```
ps -ef | grep "detect"
```

```
ps -ef | grep "vigilent"
```

```
ps -ef | grep "auditd"
```

If the services are not running, restart the services.

To restart the **vigilent** process, go to the `- /usr/netiq/pssetup` directory and run the following command:

```
./vigilentagent.rc restart
```

To restart the **detectd** process, go to the `- /usr/netiq/pssetup` directory and run the following command:

```
./detectd.rc restart
```

To restart the **auditd** process, go to the - `/usr/netiq/pssetup` directory run the following command:

```
service auditd restart
```

Change Guardian Policy Editor Not Working

NOTE: This issue is applicable if you are using the Agent to monitor Change Guardian server.

Issue: The policies are not applied to the Agent after it is assigned in Policy editor.

Workaround: To verify whether the policies are applied to the Agent after they are assigned in Policy Editor, check if the `<rule>.xml` file is created on the computer in the following directory:

```
/usr/netiq/vsau/etc/detectd.d/groups/<platformauditobject>/rules/
```

Auditing Not Working

Issue: The events are not generated even though all the configuration settings are successful.

Workaround: Verify if the spool file entry is frequently updated when events are not generated even though all the configuration settings are successful in the following directory:

```
/usr/netiq/vsau/local/spool/LinuxAuditObject__singleton/*.udetect_events
```

Agent Status is DOWN in UNIX Agent Manager

Issue: The status of the Agent is down because of following reasons:

- Agent not installed successfully
- Agent services are not running
- Firewall rules are not functioning

Workaround: Ensure that you have installed the Agent successfully and the corresponding services are running. Check the firewall settings, and ensure that port 2620 is open.

Events Not Generated When Write Permissions Are Modified

Issue: When you modify the write permission corresponding to rule group and others of a file, Change Guardian fails to generate events for file monitoring.

Workaround: NetIQ recommends that you do not modify the file permissions.

UNIX Agent Manager displays Agent Status as *Auth Error*

Issue: UNIX Agent Manager displays the following host status

```
Auth Error
```

in the following scenarios:

- After adding the host to UNIX Agent Manager during upgrade to version 7.5.

  Retain the credentials from UNIX Agent Manager 7.4.

  NOTE: Credentials must be either custom Agent credentials or UNIX Agent Manager database credentials that you used to connect to UNIX Agent Manager 7.4.

- While adding the host to UNIX Agent Manager after successful remote Agent installation.

  Remove the host IP address or host name from the host list of UNIX Agent Manager through which you installed the Agent on that host computer earlier (if any).

Add Host Displays Error While Adding Agents

Issue: The following authentication error:

```
Unable to authenticate with the Agent on <IP_address>. Please verify the provided credentials are correct.
```

is displayed while adding same Agent to multiple UNIX Agent Manager computers.

Workaround: Retain the same credentials set via first UNIX Agent Manager that you used for connecting to the Agent.

User Browse Option Does Not Work While Creating Policies

Issue: User Browse option does not work while creating policies using Policy Editor.

Workaround: To enable browsing for UNIX data sources while creating a policy, the computer where you install the Policy Editor must have a Windows Agent. If you do not install an Agent on the Policy Editor computer, you must manually enter the data source paths while creating a policy.

For 32-bit, set the `repositoryEnabled` flag (in `\HKLM\Software\NetIQ\ChangeGuardianAgent\repositoryEnabled` directory) to `1`, and then restart the Windows Agent.

For 64-bit, set the `repositoryEnabled` flag (in `\HKLM\SOFTWARE\Wow6432Node\NetIQ\ChangeGuardianAgent\repositoryEnabled` directory) to `1`, and then restart the Windows Agent.

Agent is Unable to Send Events to Sentinel

Issue: Security Agent for UNIX is unable to send events to Sentinel server because of the certificate issue with Sentinel Agent Manager Connector.

Run the following command to check if the Agent is connected to the Sentinel via Sentinel Agent Manager connector:

```
netstat -an | grep 1590
```

If the Agent is not connected, and the communication between the Agent and Sentinel fails, following is the workaround.

Workaround: To regenerate the certificate for the Sentinel Agent Manager Connector, perform the following steps:

1. Open **Sentinel Control Center** and perform the following steps:
   a. Go to **Event Source Management** window, right-click the **Agent Manager**.
   b. Click **Edit**.
   c. Go to **Security** tab, and select **Custom** under **Server Key Pair** setting.
   d. Click **OK**.
2. Right-click the **Agent Manager** again and perform the following steps:
   a. Click **Edit**.
   b. Go to **Security** tab and select **Internal (default)** under **Server Key Pair** setting.
   c. Click **OK**, and close the **Event Source Management** window.

   The Sentinel Connector Agent Manager Connector certificate is regenerated.
3. Restart the Agent by running the command:

   ```
   /usr/netiq/pssetup/vigilentagent.rc restart
   ```

A Managing Security Agent for UNIX Services

This chapter describes various key processes that, are used to validate the Agent services installation and restart methods used for starting and stopping the Agent services.

Validating Agent Services Installation

The following are key processes used by Security Agent for UNIX to validate the Agent services installation:

Key process	Description
VigilEntAgent	UNIX Agent Manager uses this process to communicate with the common components of the Agent. This process should run continuously after the Agent is installed. Agent also uses this process to run security checks and perform baselining for Sentinel, Change Guardian, and Secure Configuration Manager.
detectd	Sentinel and Change Guardian use this process to perform monitoring tasks and data retrieval. The behavior of this process is directed by the content of the `detect.xml` file.
uvserv	Secure Configuration Manager database and the Log Management database use this process to communicate with Agent. Each connection spawns a **uvserv** process that performs the operation or sends a request to the **VigilEntAgent** process to perform the operation. The connection remains open until the requesting database receives data.
Nqmagt	This process monitors the status of the other Agent processes and restarts them if necessary. This process should run continuously after the Agent is installed.

Restart Methods for the Security Agent for UNIX

You can select the startup type to be used for starting and stopping the common components. Following is the list of the available start methods:

Option	Description
`rclink`	Starts the Agent processes immediately after the deployment process and adds a startup script to the `/etc/rc.d` directory. This startup script starts the Agent processes 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 processes immediately after the deployment process and adds an entry to the `/etc/inittab` file. This `inittab` file entry starts the Agent processes at the default run level after each reboot.
`inetd`	Starts the Secure Configuration Manager processes when needed and then stops and unloads the Agent processes. **NOTE:** `inetd` is not applicable for Sentinel and Change Guardian.