Security Agent for UNIX

Installation and Configuration Guide

October 2021

Legal Notice

Contents

About this Book

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

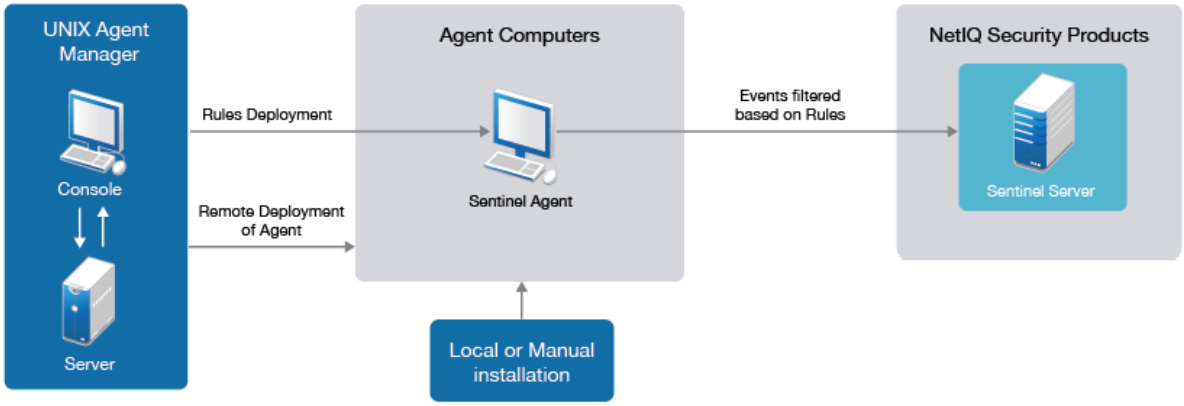
1 Understanding Security Agent for UNIX

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

- Deficits in 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

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

Figure 1-1 *Security Agent for UNIX Architecture*



You can deploy and manage Security Agent for UNIX using the following:

UNIX Agent Manager (UAM). UAM is a console and data store that you can use to manage the Security Agent for UNIX components in Sentinel. UNIX Agent Manager runs on Windows, UNIX, and Linux operating systems. Most features can be accessed from a command line as well as the console.

The following tables list the functionalities of UAM:

Table 1-1 *UAM functionality for Sentinel*

Function	UAM
Agent deployment	Performed by UAM server
Audit diagnostics	Yes
Enhanced certificate management	No
Asset view	Shows which agent components are enabled on each asset
Monitoring the agent status	Yes
Patch release	Yes for all patches
Licensing and availability	Available with a licensed instance of Sentinel

Table 1-2 *UAM for Sentinel*

Function	UAM
Remote agent installation, upgrades, reconfiguration, and uninstallation	Yes
Sentinel rule deployment	Yes
Sentinel Oracle endpoint management	Yes

When you install an agent, you can choose the security product as Sentinel, which monitors the computer on which the agent resides. A single agent can perform monitoring of the security product Sentinel. Sentinel has its own method for registering the agents and configuring the agent to send the proper data. This security product Sentinel is referred to as the agent component.

For Sentinel, you must deploy rules on the Sentinel Agent by using UAM. 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.

2 Planning Your Security Agent for UNIX Installation

This chapter provides information about planning the agent installation. This chapter assumes that you have Sentinel installed on your computer.

Implementation Checklist

Use the following checklist to plan and install the agent:

❑	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 for Security Agent for UNIX.
❑	Install the security product you want to use with the Agent. If you are using Sentinel, install the Agent Manager Connector as well.
❑	Depending on your Agent deployment requirements, determine whether you need to install UAM. For more information, see Table 1-1, "UAM functionality for Sentinel," on page 10.
❑	Review the deployment considerations to understand how you can install, upgrade, and manage agents. For more information, see "Deployment Considerations" on page 12.
❑	Install the Agent on the computer you want to monitor. ◆ For information about installing using an answer file, see "Silent Installation" on page 19.
❑	Ensure that the audit service is running on the Agent without any interruption. For more information see, "Validating Agent Services Installation" on page 59.
❑	(Conditional) For Sentinel, deploy Sentinel rules using UAM 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 27.

Understanding License Information

This section provides licensing information for 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 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 or the associated End User License Agreement (EULA).

System Requirements

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

Deployment Considerations

This section provides an overview of the most important considerations for installing or upgrading Security Agent for UNIX.

For varied Security Agent for Unix deployment configurations, refer Table 2-2 for recommended agent management tools and procedures.

Table 2-1 *Install or Upgrade for Individual Products and Product Combinations*

Agents and Deployment Configuration	Tool Required for New Installation or Upgrade
Sentinel	UAM

Understanding FIPS 140-2 Implementation

Security product, Sentinel supports Federal Information Processing Standard (FIPS) 140-2 communication among the product components. You can configure the UAM, Security Agent for UNIX, and Sentinel 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.

IMPORTANT

- If UAM is in FIPS mode, you cannot deploy Security Agents for UNIX in FIPS or non-FIPS modes.
- If both, UAM and the target operating system are not in FIPS modes, deployment of Security Agent for UNIX in FIPS mode succeeds.
- If the target operating system is in FIPS mode, UAM cannot deploy Security Agent for UNIX in FIPS or non-FIPS modes.
- If UAM is in non-FIPS mode, you cannot convert it to FIPS mode, during an upgrade.

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.

UAM uses Mozilla NSS libraries and Java SSL libraries for creating the listener on port 2222 and OpenSSL libraries for communicating with Agents. For UAM, 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 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 to non-FIPS mode.

Tasks	For more information, see…
Remote installation: To enable the Agent in FIPS 140-2 mode during remote installation	"Installing the Agent Using UAM" on page 17

FIPS-Enabled Components

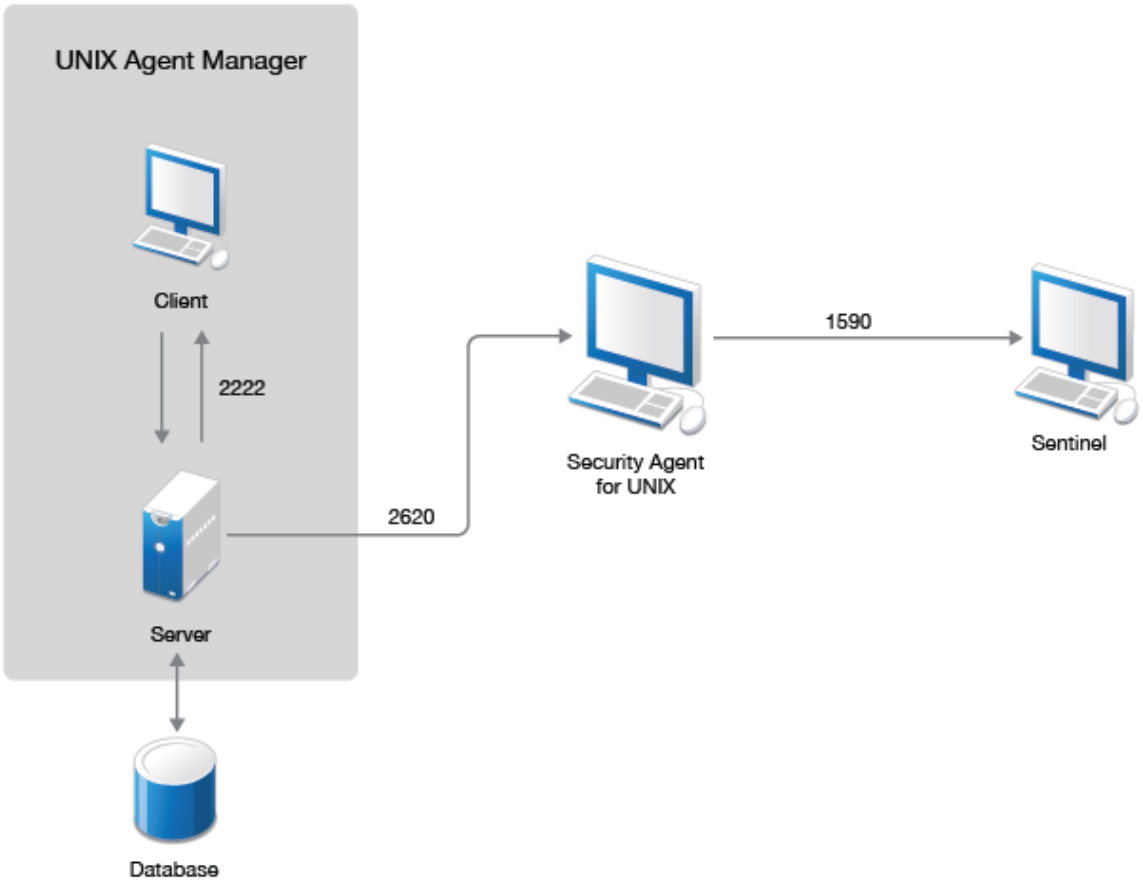
The following components provide FIPS 140-2 support:

- Sentinel Server 7.4 and later
- Sentinel Security Agent for UNIX 7.5 and later
- UAM 7.5 and later
- Sentinel Agent Manager Connector 2011.1r5 and later

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 UAM
1590	Communication with Sentinel
2222	Communication between UAM client and UAM server

3 Installing Security Agent for UNIX

You can install the agent in the following ways:

- Remote installation: Remote installation provides a convenient and uniform method for installing one or more agents.

  You can install the agent remotely by using UAM. Depending on your agent deployment requirements, you can decide whether you need to install UAM. For more information, see Table 1-1, “UAM functionality for Sentinel,” on page 10.

  - Remote installation using UAM

    You can use the Deployment wizard provided in the UAM 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.
- Local installation using command line: Local installation guides you through logging on to an agent computer and locally installing all required components on the system running the agent
- 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.

This chapter provides information about the following topics:

Installation Using UAM

This section includes the following topics:

NOTE: UAM 7.5 and later are not compatible with AppManager Agent for UNIX.

Installing UAM

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

After you have installed UAM, you can set up users and assign access to them. For more information about managing UAM users, see Chapter 4, “Managing Users Using UAM,” on page 23. The following sections guide you through installing UAM:

Installing UAM on Microsoft Windows

Complete the following steps to install the UAM server, the UAM console, or both on a Windows computer.

To install UAM 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 FIPS encrypted algorithms unless you are certain that your environment requires that restriction. If you enable FIPS 140-2 mode, UAM 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 25.

   NOTE: Remove TLS1.0 and TSL1.1 from the property `jdk.tls.disabledAlgorithms` in `<UNIX Agent Manager installation path>\jre\lib\security\java.security` file after enabling FIPS mode. Then restart the services.
3. Complete the automatic installer wizard.
4. Specify and confirm a password for the UAM server. The administrator user account must use this password.

   NOTE: To change the administrative password for the UAM 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 UAM on Linux

Complete the following steps to install the UAM server, the UAM console, or both on a Linux computer.

To install the UAM 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.

Example: `tar -zxvf UNIX_Security_Agent_tar.gz`

2 Change to the directory where you extracted the installer:

```
cd <directory_name>
```

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

Example: `tar -zxvf Linux_x86_64_UAM.tar.gz`

4 (Conditional) Enable FIPS mode:

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

NOTE: Do not restrict communication security settings to FIPS encrypted algorithms unless you are certain that your environment requires that restriction. If you enable FIPS 140-2 mode, UAM 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 25.

NOTE: Remove TLS1.0 and TSL1.1 from the property `jdk.tls.disabledAlgorithms` in `<UNIX Agent Manager installation path>\jre\lib\security\java.security` file after enabling FIPS mode. Then restart the services.

---

5 Specify the following command to install the UAM in the new UAM folder:

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

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

7 Create the UAM database and set the administrator password before you run the `run.sh` script:

```
./runserver.sh
```

8 Start the UAM console:

```
./run.sh
```

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

Installing the Agent Using UAM

To remotely deploy the agent components:

1 Install and launch UAM. For more information, see "Installing UAM" on page 16.

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 check box 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 one or more hosts and want to use them, select **Add the selected components to the existing install** in the **Installation type**.

8 (Conditional) If you are newly installing the components on one or more hosts, select **Create a new install with the selected components** in the **Installation type**. This removes any components already installed on the hosts, 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 FIPS encrypted algorithms unless you are certain that your environment requires that restriction. If you enable FIPS 140-2 mode, UAM 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 25.

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 59.

12 (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**.

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

14 (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 UAM, 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 Enter the UAM database account **Username** and **Password**.

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

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 UAM on the system running the agent. For information about how to deploy rules, see "Activating Rule Sets" on page 33.
- 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`.

Parameter	Description
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.
IQCONNECT_PORT	Specifies the port that the agent uses to listen for communications from UAM. 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 59. Valid entries are rclink and inittab. The default option is rclink.
USE__COMMON	Specifies whether the agent communicates with UAM in FIPS mode. For more information about this option, see Chapter 5, "Converting Agent from Non-FIPS to FIPS mode," on page 25. 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 uses to communicate with Sentinel. The default value is 1590.
SENTINEL_FAILOVER1_ADDR=	Specifies the IP address of the failover Sentinel that the agent attempts to contact if the primary Sentinel does not respond.
SENTINEL_FAILOVER1_PORT=	Specifies the port that the agent uses 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 attempts to contact if the first failover Sentinel does not respond.
SENTINEL_FAILOVER2_PORT=	Specifies the port that the agent uses 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 monitors 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 stops monitoring.

Parameter	Description
SENTINEL_STARTUP	Specifies restart method for the agent. For information about the options, see "Restart Methods for the Security Agent for UNIX" on page 59. 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 deletes 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 UAM

UAM allows administrators to control user access to features and computers. To log on to any UAM server, an administrator on that server must create the user account in the UAM 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 to users:

1. Log on to UAM console as an administrator
2. Click **Access Control** > **Admin Console**.
3. Add the users that need access to that UAM server, then assign the appropriate permissions that are listed in the **Permissions** tab.

Configuring the UAM Server

UAM 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 UAM server. This functionality is not available if UAM is installed in FIPS mode.

- "Configure to Use LDAP or Active Directory" on page 23
- "Configure to Use SSL with LDAP or Active Directory" on page 24

Configure to Use LDAP or Active Directory

To configure the UAM server to use LDAP or Microsoft Active Directory credentials.

Prerequisites

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 UAM server can use to access the LDAP or Active Directory server

To configure UAM server to use LDAP or Active Directory credentials:

1. Log on to UAM as an administrator, and open the **Manage Server** window.
2. Click **LDAP** and then click **Add** button.
3. 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 UAM.

4. Select the domain and provide information as requested on the window using the following guidelines:
   - **4a** In **Server Address**, enter the LDAP or Active Directory server computer name and port. For example, `ldap://<ldap_ip_address>:389`
   - **4b** In **User's Parent DN**, enter the path to the node that contains the user name. For example, `ou=AMAdmins,dc=netiq,dn=com`
   - **4c** In **Username**, enter the attribute you want UAM 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 UAM is `uid`.
   - **4d** (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`.
5. Click **Refresh Users**.

Configure to Use SSL with LDAP or Active Directory

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

1. 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 UAM using the **Manage Server** window where you identify your LDAP server.
2. Close and restart the UAM after you import the certificate.

NOTE: For more information about LDAP authentication, see Logging in by Using LDAP User Credentials in *The 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. Change the log level from 1 to 4 in `/etc/vigilent.conf` file to see the logs.
4. 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 59.

   ---

5. 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 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 7, “Understanding Security Rules for Sentinel,” on page 31.

Configuring the Agent with Oracle

If you use Sentinel to monitor Oracle on UNIX or Linux, you must use UAM 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 UAM 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**:
   - 5a **User Name**: Enter the Oracle user name that has Database Administrator (DBA) permissions.
6. Click **Register Endpoints**.
7. Activate the Oracle rule set. For more information about activating rule sets, see “Deploying Rule Sets” on page 27.

Deploying Rule Sets

Complete the following steps to activate the rule set delivered with the latest version of UAM 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 UAM.
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

Enabling process accounting enhances security event reporting in Sentinel. However enabling process accounting substantially increases the activity on the monitored computer and also changes the base computer configuration. Therefore, it is not recommended to enable process accounting unless it is acceptable for your environment.

Do not enable process accounting if syslog reports those events that you want to monitor.

To enable process accounting:

1 Deploy Process Accounting rule sets to the agent.

This sets the event source configuration parameter `start_process_accounting` to `1`.

2 Start the `psacct` service in the Sentinel server.

Disabling Process Accounting

Disable process accounting if you do not want to have an increased activity on the monitored computer or when you do not want the base computer configuration to change.

To disable process accounting:

1 In UAM, set the event source configuration parameter, `start_process_accounting` to `0`.

2 Redeploy Process Accounting rule sets to the agent.

3 Stop the `psacct` service in the Sentinel server.

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 UAM. This rule group contains rules that process Oracle audit events.

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

7 Understanding Security Rules for Sentinel

This chapter provides an overview of Agent rules and how to implement them using the UAM.

You can access Rules Manager in UAM 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.

UAM 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 UAM server, and can be accessed by any UAM 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 UAM if this is an initial implementation of rule sets in your organization. The UAM 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 32

Viewing Rule Sets and Editing Rule Set Properties

When you open a rule set, the UAM 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 34.
- Rule groups provide editable properties at the group level, and contain individual rules. For more information, see “Understanding Rule Groups” on page 35.
- 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 36

UAM 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:

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 UAM.
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

UAM 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:

1. Click **Edit Rule Set** in **Rules Management** screen, then click **Wizard** > **Rule Wizard**
2. Follow the prompt to complete the steps.

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 36.
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 36
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:

1. Right-click **Rule Set**
2. Click **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 36
Initialization code	“Understanding Initialization Code” on page 37
Main code	“Understanding Main Code” on page 39
Conditionals (And and Or objects)	“Understanding Conditionals and Comparisons” on page 37
Comparisons	“Understanding Conditionals and Comparisons” on page 37
Time conditions	“Understanding Time Conditions” on page 38
Templates	Templates contain information for the Rule wizard. Template nodes do not require user maintenance.

The UAM 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 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 39.

Rules that contain a comparison that is not a child element of an And or Or comparison is not a conditional comparison. 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 UAM displays when the associated rule is active.

To change the schedule of a rule governed by a time condition:

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.

To delete time conditions:

1. Right-click the time condition node you want to delete, and 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**.

UAM 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.

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 UAM computer and activate the modified rule set on remote Agent computers. For more information about activating rule set see, "Activating Rule Sets" on page 33.

Adding New Main Code

UAM 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 UAM computer and activate the modified rule set on remote Agent computers. For more information, see "Activating Rule Sets" on page 33.

Deleting Main Code

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

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

UAM 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

UAM uses parameter aliases to make parameters generated by event sources or rules easier to understand. UAM 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

UAM uses hide node name underscores to hide underscores in rule set, rule group, and parameters.

Deciding Whether to Use Hide Node Titles

UAM 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"`

Commands	Description
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.

To create a Rule Group for Stash or BitBucket to be 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.

8 Managing Security Agent for UNIX Configuration

To configure Security Agent for UNIX prior to 7.5 versions, you must use UAM only.

You can reconfigure the parameters when you want to modify the configuration settings after an upgrade or a new installation.

Managing Agent Configuration in UAM

You can use UAM to configure the parameters for managing the following security product:

- Sentinel

Perform the following procedure:

1. Launch UAM console.
2. For monitoring Sentinel servers, navigate 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**.

9 Upgrading Security Agent for UNIX

To upgrade the Security Agent for UNIX you can use UAM.

This chapter includes the following topics:

Upgrading Using UAM

UAM provides a console to upgrade existing agents. You must first upgrade the UAM before upgrading your agents.

This section contains the following topics:

Upgrading UAM

This section contains the following topics:

Backing Up Agent Information to File

The UAM server stores information about all the agents you monitor; this information can also be exported to a file. You must back up this information before any activity that might affect your UAM server, such as an upgrade. A backup is also useful in situations when you want to move UAM to another computer.

To export your Agent list and configuration information, click **Manage Hosts > Export/Import Host Lists** in UAM.

Due to security improvements introduced in 7.5.0, UAM 7.5.0 and later can only manage Security Agent for UNIX 7.5.0 and later. To manage older agents until you upgrade them, retain an instance of UAM prior to 7.5.0.

To export agent information from UAM:

1. In the left pane of UAM, 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 UAM.

Upgrading UAM on Linux

Perform the following steps to upgrade UAM on Linux.

To upgrade UAM on Linux:

1 Close all UAM applications.

2 Download the UAM installer from the Patch Finder website.

3 Extract the compressed installer file to the computer where you want to install UAM.

4 Start the upgrade:

```
./installserver.sh upgrade
```

5 When prompted, specify the path of the UAM database where the current UAM database folder exists.

Example: `<UAM Directory>/UAM/UAMDB`

6 Replace the associated UAM certificates, once the upgrade completes.

7 Start UAM:

```
./run.sh
```

8 Log in as an `admin` user configured during the previous UAM Linux installation version.

UAM launches successfully with pre-configured agents.

Upgrading UAM on Microsoft Windows

To upgrade UAM on Windows, perform the following steps.

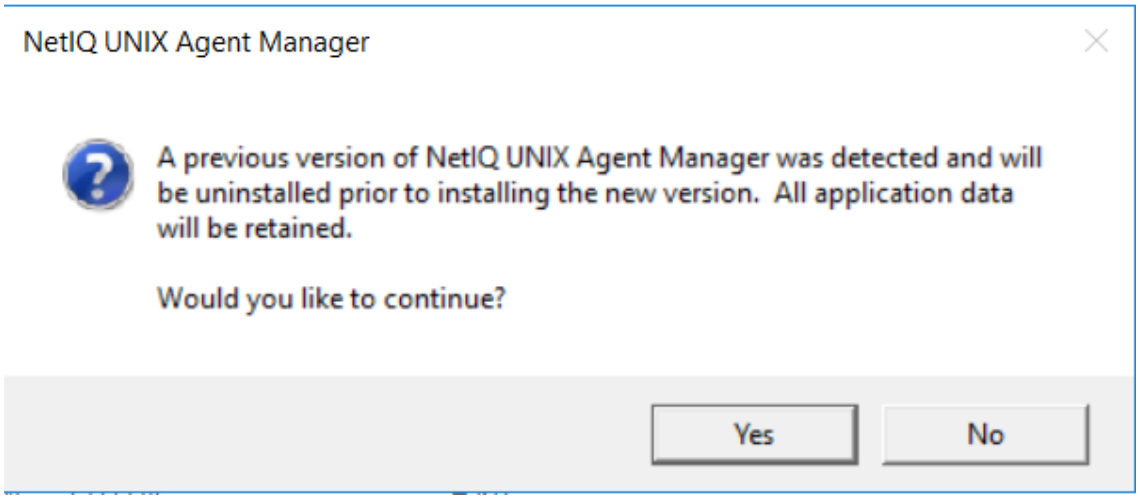
To upgrade UAM on Microsoft Windows:

1 Download the UAM installer from the Patch Finder website.

2 Extract the compressed installer file to the computer where you want to install UAM.

3 Run the UAM installer.

Figure 9-1 *Uninstallation of Older Version*



Continue by selecting **Yes**. Complete further steps and finish the installation.

4 Replace the associated UAM certificates, once the upgrade completes.

Applying Patches

This section is applicable if you are using UAM.

Patches to the Agent are available in a zipped file known as a p-ball. Patches to UAM are applied to the UAM server, which automatically applies any required changes to the consoles using that server. To update UAM on Windows, click **Update UNIX Agent Manager** on the Start menu. To update UAM on Linux, run the `update.sh` command.

Appying a Patch Using UAM

To apply a patch on the agent using UAM, perform the following steps.

To apply a patch using the UAM:

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.

Applying a Patch Manually

To apply a patch manually, perform the following steps.

To apply a patch to the Agent computer manually:

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.

Upgrading Manually

You can upgrade Security Agent for UNIX using UAM or manually.

Upgrading using UAM

To upgrade the Security Agent using UAM, perform the following steps.

To upgrade the agent:

1 In UAM, select the hosts that you want to upgrade.

2 Go to **Manage Hosts > Upgrade Hosts**.

3 Select **Upgrade Security Components**.

4 Click **Start Upgrade**.

Upgrading Manually

To manually upgrade the agent, perform the following tasks.

To Upgrade an agent on a local computer:

1 Download agent artifacts and certificates. See, the Micro Focus Downloads page.

2 Log on to an Agent computer using an account with superuser privileges.

3 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.

4 Change to the directory where you extracted the installer:

```
cd <directory_name>
```

5 Start the install script:

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

6 To upgrade, 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?
```

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 security software. 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 59.
11. (Conditional) To install newer components in additional, see Chapter 3, "Installing Security Agent for UNIX," on page 15.
12. The installation process finishes and the Agent starts. It might take a few minutes for all services to start after installation.

10 Uninstalling Security Agent for UNIX

You can use UAM 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 security products.

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

This chapter includes the following topics:

Uninstalling Security Agent for UNIX Locally

To uninstall the Agent locally, go to the installation directory, then run the following command as a `root` user:

```
./uninstall.sh
```

Uninstalling Security Agent for UNIX Using UAM

You can use the UAM console to uninstall the agents. This option allows you to uninstall the agent from many computers together.

Use the following steps to uninstall the agent using UAM:

1. Select the computers from which you want to uninstall the Agent.
2. Click **Manage Hosts** > **Uninstall Agent**.

Uninstalling UAM

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

NOTE: If require remove/delete the DB in Windows after you uninstall UAM. Remove the content of `C:\Program Files (x86)\NetIQ\UNIX Agent Manager\`

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

```
installserver.sh remove
```

When you have completed the uninstall program, you can remove the UAM directory by running the following command:

`rm -rf UAM`.

Verifying Uninstallation of the Security Agent for UNIX

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 UAM, 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.

11 Troubleshooting

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

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, run the following command:

```
service auditd restart
```

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 UAM

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.

UAM displays Agent Status as *Auth Error*

Issue: UAM displays the following host status:

```
Auth Error
```

in the following scenarios:

- After adding the host to UAM during upgrade to version 7.5.

  Retain the credentials from UAM 7.4.

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

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

  Remove the host IP address or host name from the host list of UAM 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 UAM computers.

Workaround: Retain the same credentials set via first UAM that you used for connecting to the 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
   ```

Agent Displays An Error While Connecting to Sentinel

Issue: The following error:

```
post of events failed to https://sentinel.demo.local:1590/events: ##
```

occurs in the `/var/log/messages` location on the Agent while connecting to Sentinel.

Workaround: Perform the following procedure:

1. Check the Sentinel configuration IP address for `SENTINEL_DESTINATIONS` flag in `/etc/vsaunix.cfg` configuration file.

   If the IP address is incorrect, provide the correct IP address.
2. Run the following commands to check whether the **detectd** and **vigilent** services are running.

   ```
   ps -ef | grep "detect"
   ps -ef | grep "vigilent"
   ```
3. (Conditional) If **detectd** and **vigilent** services are not running, restart the services. Run the following commands:

```
/etc/init.d/detectd restart
/etc/init.d/vigilentagent restart
```

4 (Conditional) If the **detectd** and **vigilent** services are running, check connection status. Run the following command:

```
netstat -na | grep 1590
```

Wait for a few seconds and check the connection status again.

If there is any certificate related issue, refer to *Sentinel Agent Manager* documentation.

12 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`	UAM 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.
`detectd`	Sentinel 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.
`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.