User Guide

NetIQ® Change Guardian™ Product

March 2014

Legal Notice

Contents

About this Book and the Library

The *User Guide* provides planning, installation, and conceptual information about the Change Guardian Policy Editor, the Change Guardian server, and Change Guardian modules. This book guides you through installation, defines terminology, and explains implementation scenarios.

Intended Audience

This book provides information for individuals responsible for understanding Change Guardian product concepts, and for individuals installing and using this operational change auditing solution for their enterprise network.

Other Information in the Library

The library provides the following information resources:

Help

Provides context-sensitive information and guidance for frequently- performed-tasks.

Release Notes

Provides additional information about the release, known issues, and resolved issues.

Conventions

The library uses consistent conventions to help you identify items throughout the documentation. The following table summarizes these conventions.

Convention	Use
Bold	◆ Window and menu items ◆ Technical terms, when introduced
Italics	◆ Book and CD-ROM titles ◆ Variable names and values ◆ Emphasized words
`Fixed Font`	◆ File and folder names ◆ Commands and code examples ◆ Text you must type ◆ Text (output) displayed in the command-line interface
Brackets, such as *[value*]	◆ Optional parameters of a command
Braces, such as {*value}*	◆ Required parameters of a command
Logical OR, such as *value1*|*value2*	◆ Exclusive parameters. Choose one parameter.

About NetIQ Corporation

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

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

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

Enabling critical business services, better and faster

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

Our Philosophy

Selling intelligent solutions, not just software

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

Driving your success is our passion

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

Our Solutions

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

Contacting Sales Support

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

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

Contacting Technical Support

For specific product issues, contact our Technical Support team.

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

Contacting Documentation Support

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

Contacting the Online User Community

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

1 Introduction

Every day, organizations face increased information security risks when privileged users make unauthorized changes to critical files, systems, and applications within their IT infrastructures.

NetIQ Change Guardian monitors critical files, systems, and applications in real-time to detect unauthorized privileged-user activity, helping you significantly reduce organizational risk to critical assets. It also helps you achieve compliance with regulatory and privacy standards, such as the Payment Card Industry Data Security Standards (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA), the International Organization for Standardization's latest standards (ISO/IEC 27001), and others.

1.1 What is Change Guardian?

NetIQ Change Guardian gives you the security intelligence you need to rapidly identify and respond to privileged-user activities that could signal a security breach or result in compliance gaps. It helps security teams detect and respond to potential threats in real-time through intelligent alerting of authorized and unauthorized access and changes to critical files, systems, and applications.

To combat an increasingly sophisticated threat landscape and complex computing environment driven by such technologies as BYOD, mobility and cloud, organizations must take a layered and integrated approach to defending their critical systems and sensitive data. NetIQ Change Guardian products provide the following essential protection measures:

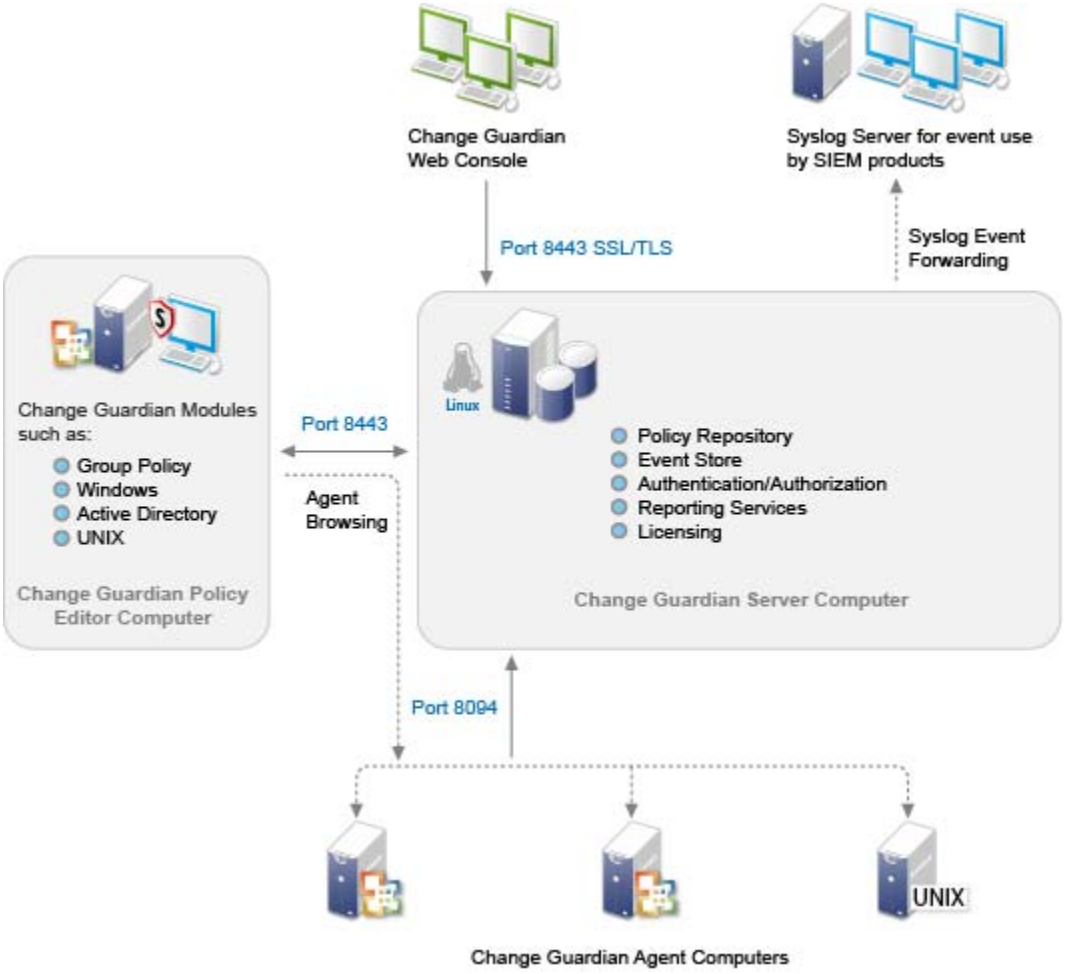
- **Privileged-user monitoring** - Audits and monitors the activities of privileged users to reduce the risk of insider attacks.
- **Real-time change monitoring** - Identifies and reports on changes to critical files, platforms and systems to help prevent breaches and ensure policy compliance.
- **Real-time intelligent alerting** - Provides immediate visibility to unauthorized changes that could lead to a breach, enabling the fastest threat response.
- **Compliance and best practices attainment** - Helps satisfy compliance mandates by demonstrating the ability to monitor access to critical files and data.

By centrally recording and auditing changes, creating intuitive monitoring policies through policy-based monitoring, and automating daily change auditing and reporting, Change Guardian helps you to avoid the time and complexity required to analyze disparate platform logs.

NetIQ Change Guardian also integrates seamlessly with your existing security information and event management (SIEM) solution, such as NetIQ Sentinel, to extend its ability to detect and respond to threats by pinpointing the who, what, when, and where of an event while providing before and after values. Armed with this comprehensive security intelligence, you will be better able to mitigate the impact of an attack before serious damage or compliance gaps can occur.

1.2 How Change Guardian Works

Change Guardian includes a number of software components that you should plan to install strategically over a number of computers.



Change Guardian comprises the following components:

Change Guardian Policy Editor A Windows-based console through which you create and deploy policies to monitor critical files, systems, and applications in your enterprise.

Change Guardian Server A Linux-based computer that stores your policies and change events.

Change Guardian Web Console A web console that allows you to monitor security event detail that pinpoints the who, what, when, where, and authorization status of a change or activity, including before- and after- details of the change.

Agents Platform-specific software on Windows and UNIX computers that allow you to forward events to the Change Guardian server based on policies you have deployed. Opening ports on agent computers is not necessary unless you want the ability to browse the computer for files, processes, and users when you create policies.

The Change Guardian server uses several ports for internal and external communication. Ensure that you open the appropriate ports for your environment.

Component	Ports	Direction	Required /Optional	Description
Policy Editor Console	8443	Outbound	Required	Connecting to the Change Guardian server for the following actions: ◆ remote object browsing to Windows-based monitored assets ◆ configuring email in Change Guardian or Sentinel ◆ updating policies to the Change Guardian server
	2620	Outbound	Optional	Allows remote object browsing to UNIX-based monitored assets.
	389 or 636	Outbound	Optional	Allows remote object browsing to Active Directory.
Change Guardian Server	8094	Inbound	Required	Allows the Change Guardian server to accept connections from agents that are retrieving their assigned monitoring policies.
	8443	Inbound	Required	Allows the Change Guardian server to receive events from monitored assets. **NOTE:** This port may not be needed if you are sending events from monitored assets to an alternate destination.
	389 or 636	Outbound	Required	Enables the LDAP authentication and the expansion of Active Directory groups. The port initiates a connection to the LDAP server.
	25	Outbound	Optional	Default email port. This port may be different based on the specific email implementation.
	54984	Inbound	Optional	Used by the Sentinel Appliance Management Console (WebYaST). Also used by the Sentinel appliance for the update service.
	443 or 80	Outbound	Optional	WebYaST initiates a connection to either the NetIQ appliance update repository (https://nu.novell.com) or a Subscription Management Tool Service location on your network.
Windows Monitoring Agents	8094	Outbound	Required	Allows the agent to connect to the Change Guardian server to retrieve assigned monitoring policies.
	8094	Inbound	Optional	Allows the Policy Editor to connect to the agent to browse objects on the monitored asset.
	8443	Outbound	Required	Allows the agent to connect to the Change Guardian server or Sentinel to send events.
UNIX Monitoring Agents	8094	Outbound	Required	Allows the agent to connect to the Change Guardian server to retrieve assigned monitoring policies.
	2620	Inbound	Optional	Allows the Policy Editor to connect to the agent to browse objects on the monitored asset.
	8443	Outbound	Required	Allows the agent to connect to the Change Guardian server or Sentinel to send events.

Component	Ports	Direction	Required /Optional	Description
UNIX Agent Manager	2620	Outbound	Required	Allows the UNIX Agent Manager to connect to a UNIX agent to get status and diagnostic information.
	2222	Outbound	Required	Allows the UNIX Agent Manager client to connect with the UNIX Agent Manager server.
	22	Outbound	One of these is required.	(SSH) UNIX Agent Manager requires SSH+SFTP or Telnet+FTP access to computers targeted for remote agent deployment.
	21/23	Outbound		(Telnet/FTP) UNIX Agent Manager requires SSH+SFTP or Telnet+FTP access to computers targeted for remote agent deployment.

1.3 Managing Event Destinations

If you are using Change Guardian as a standalone product, the default event destination sends asset events to the Change Guardian server so you can view access and changes to critical files, systems, and applications. You can use Change Guardian to extend the broader event collection and real-time analytic capability of a SIEM solution by adding event destinations to send asset and Change Guardian system events to NetIQ Sentinel or a third-party SIEM in your environment. You can also send Change Guardian system events to an existing syslog server in your environment.

1.3.1 Adding Event Destinations

Change Guardian allows you to customize where you send asset and Change Guardian system events based on your environment and regulatory needs by creating event destinations. Once you have created event destinations, you can further define where events are sent by assigning one or more event destinations to each Change Guardian policy.

To add event destinations:

1. Log in to the Change Guardian Policy Editor.
2. Select **Settings > Event Destinations**.
3. Click **Add**.
4. Specify a unique name for the event destination.
5. Specify one of the following event destination models:
   - REST Dispatcher

     Use this model to send asset and Change Guardian system events to your Sentinel server.
   - Syslog Dispatcher

     Use this model to send Change Guardian system events to a third-party SIEM or syslog server in your environment.

     If you change the default event destination, all new policies will automatically send event data to the new default location. Existing policies will continue to use the event destination default from the time they were created. To change the event destinations for existing policies, see "Assigning Event Destinations to Policies" on page 15.
6. Provide a descriptive statement about the purpose of the event destination.
7. Provide system information for the server where you want to send events.

8 If you want to send Change Guardian system events that only match specific criteria, select the checkbox and provide filter criteria.

   Change Guardian uses the Lucene query language for filtering events. For more information, see Apache Lucene - Query Parser Syntax.

9 Click **OK**.

1.3.2 Assigning Event Destinations to Policies

By default, asset event data is sent to the Change Guardian server. If you want to send this data to the Sentinel server, you must add the new event destination to each policy set or policy. The new event destination will take effect at the next heartbeat interval when the updated policy information is read by the asset computer.

To assign event destinations to a policy:

1 Log in to the Change Guardian Policy Editor.

2 Click **Policy Assignment**.

3 Select an asset group or computer, and click **Assign Policies**.

4 Select a policy set or policy and click **Advanced**.

5 Select the event destinations you want to use for the specified policy or policy set. You can specify more than one event destination.

   If you remove the default REST Dispatcher event destination, asset computers will no longer send event data to the Change Guardian server.

6 Click **OK**.

1.4 Change Guardian Implementation Checklist

Change Guardian installation requires you to perform the following actions:

	Checklist Items
❑	If you have purchased Change Guardian, ensure you have the following license keys: ◆ Change Guardian Server ◆ Change Guardian Module Keys ◆ NCC channel registration codes (Only for appliance installations) If you have not yet purchased Change Guardian, you may use the 90 day built-in trial license. For more information about license keys, see your Sales Associate.
❑	Determine whether you want to perform a traditional or appliance installation of the Change Guardian server. For more information see, Chapter 2, “Installing the Change Guardian Server,” on page 17.
❑	Install the Change Guardian server. ◆ If you want to perform a traditional installation, see Section 2.2, “Traditional Change Guardian Server Installation,” on page 19. ◆ If you want to perform an appliance installation, see Section 2.3, “Appliance Change Guardian Server Installation,” on page 21.

	Checklist Items
❑	Ensure the Change Guardian server is up and running by issuing the following command: `netstat -an | grep LISTEN | grep 8443`
❑	Synchronize the time on your Change Guardian server and monitored computers by using the Network Time Protocol (NTP).
❑	Verify the Change Guardian Web console can connect to the server by specifying the following URL in your Web browser: `https://`*IP_Address_Change_Guardian_server*`:8443`
❑	Install the Change Guardian Policy Editor. For more information, see Section 3.2, “Installing the Policy Editor,” on page 27.
❑	(Conditional) If you want to monitor events on UNIX computers, install UNIX Agent Manager and the UNIX agent. For more information, see Chapter 4, “Installing and Using the UNIX Agent and UNIX Agent Manager,” on page 29.
❑	(Conditional) If you want to monitor events on Windows computers, install the Windows agent. For more information, see Chapter 3, “Installing the Change Guardian Windows Components,” on page 27.

2 Installing the Change Guardian Server

This chapter guides you through planning and installing the Change Guardian server. The Change Guardian server provides policy and event storage and communication with monitored computers and systems to which you want to forward events. For more information, see Section 1.2, "How Change Guardian Works," on page 12.

Install the Change Guardian server on your own Linux-based server, or you can choose to deploy a ready-to-run appliance.

2.1 Planning for Change Guardian Server Installation

Use the checklist to verify hardware and software requirements, plan resources needed for your Change Guardian implementation, guide installation of Change Guardian components, and check connectivity following installation.

2.1.1 Supported Operating Systems and Platforms

You can install the Change Guardian server on a computer running one of the following operating systems:

- SUSE Linux Enterprise Server (SLES) 11 Service Pack 2 (64-bit)
- Red Hat Enterprise Linux for Servers (RHEL) 6.*x* (64-bit)

NOTE: Open Enterprise Server (OpenSuSE) installations of SLES do not support the Change Guardian server.

You can run the Web console on the following supported browsers

- Firefox version 5 to version 18
- Internet Explorer 8, 9, and 10

NOTE: If the Internet Security Level is set to High, a blank page appears after logging in to Sentinel and the file download pop-up might be blocked by the browser. To work around this issue, you need to first set the security level to Medium-high and then change to Custom level as follows:

1. Navigate to **Tools** > **Internet Options** > **Security** tab and set the security level to Medium-high.
2. Make sure that the **Tools** > **Compatibility View** option is not selected.
3. Navigate to **Tools** > **Internet Options** > **Security** tab> **Custom Level**, then scroll down to the Downloads section and select **Enable** under the Automatic prompting for file downloads option.

2.1.2 Hardware Requirements

The hardware recommendations for the Change Guardian server can vary based on your environment and monitoring needs. Consult NetIQ Professional Services prior to finalizing the Change Guardian implementation.

The following hardware requirements are for running the Change Guardian server in a production environment as an all-in-one Change Guardian environment:

Category	250 Monitored Assets	1000 Monitored Assets	2000 Monitored Assets
CPU	One Intel Xeon 3-GHz (4 core) CPU	Two Intel Xeon 3-GHz (4 core) CPUs (8 cores total)	Two Intel Xeon 3-GHz (8 core) CPUs (16 cores total)
Memory	16 GB	32 GB	64 GB

NOTE: The Change Guardian server is supported on x86 (64-bit) Intel Xeon and AMD Opteron processors but is not supported on pure 64-bit processors like Itanium.

2.1.3 Calculating the Server Storage Needs

The Change Guardian server stores raw data to comply with legal and other requirements. The system can be set up to use both local and network storage. Local storage has a better performance characteristics for searching and reporting while network storage provides a better compression ratio reducing the cost of storage. Change Guardian will automatically manage data between local and network storage as it ages in the system.

To determine the amount of storage required, first estimate how many days of history you need available in the system. Then determine the average number of days that are generally used for searches and reports for day to day needs. Using the following formulas, plan enough local storage for your day-to-day needs and network storage for the remainder of the history.

NOTE: Ensure that the file system partition containing /var/opt has been allocated sufficient storage based on the local storage calculation below.

Use the following formulas to estimate the amount of space required to store data:

Local event storage (partially compressed):

```
{bytes per event} x {events per second} x 0.00008 = {GB local storage per day}
({GB local storage per day} x {number of days}) x {30% buffer} = Total GB local storage
```

Networked event storage (fully compressed):

```
{bytes per event} x {events per second} x 0.00001 = {GB network storage per day}
({GB network storage per day} x {number of days}) x {20% buffer} = Total GB network storage
```

These sample recommendations model a production system that holds 90 days of online data. The recommendations assume an average event size of 1000 bytes.

Category	250 EPS	750 and 1000 EPS	1500 and 2000 EPS
Local Storage (30 days)	500 GB, 7.2k RPM drive	3x300 GB SAS, 15k RPM drives (Hardware RAID 0)	4x600 GB SAS, 15k RPM drives, (Hardware RAID 0 with 128kB stripe size)
Networked Storage (90 days)	2x128 GB	4x1 TB	8x1 TB

Storage Planning Notes:

- Plan for at least 5 days of local storage at a minimum.
- In a primarily networked storage only implementation, the amount of local storage can be minimized. However, due to decompression overhead, searching and reporting performance may be impacted by as much as 70%.
- If networked storage is enabled, event data is copied to networked storage typically after 2 days.
- Partially compressed means that the data is compressed, but the index of the data is not compressed. Fully compressed means that both the event data and index data is compressed. Event Data compression rates are typically 10:1. Index compression rates are typically 5:1. The index is used to optimize searching through the data.
- You should also plan additional hard drive space beyond your minimum requirements to account for data rates that are higher than expected.
- When configuring disk partitions larger than 2 TB on Linux, use GUID partition table (GPT) format.

2.2 Traditional Change Guardian Server Installation

You can install Change Guardian server on your own Linux server, where you own both the hardware and the full Linux operating system that is installed on your hardware. If you want to install the managed software appliance, see Section 2.3, "Appliance Change Guardian Server Installation," on page 21.

To install the Change Guardian server interactively:

1. On the command line, type the following command to extract the installation file:

   ```
   tar zxvf install_cgserver-4.1.0-xx.x86_64.tgz
   ```

2. Run the Change Guardian server installation program by typing the following command in the root of the extracted directory:

   ```
   ./install-changeguardian.sh
   ```

   NOTE: To see additional installation script options, run `./install-changeguardian.sh -h` to display the Help.

3. Press the space bar to read the license agreement. You must page through the entire agreement before you can accept it.
4. When prompted, select the standard or custom configuration.

If you select standard, installation proceeds with the 90-day Sentinel evaluation license key included with the installer. This license key activates the full set of product features for a 90-day evaluation period. At any time you can replace the evaluation license with a license key you have purchased.

5 (Conditional) If you select the custom configuration, complete the configuration using the following information:

Add a production license key: Installs a production Web console license key.

Assign admin account password: Account for global administration of the system.

Assign dbauser account password: PostgreSQL database maintenance account.

Assign appuser account password: Account used to interact with the PostgreSQL database at runtime.

Customize port assignments: Change the default ports used by the system.

Configure LDAP authentication integration: Configure an LDAP user repository to handle authentication.

Configure FIPS mode: FIPS is not currently supported.

6 Create an admin account password for global system administration.

7 Configure the server to use a static or a dynamic (DHCP) IP address. If you select to use a DHCP IP address, monitored systems must be able to resolve the hostname to connect to the Change Guardian server.

8 Create a Change Guardian `cgadmin` user password. Use this account to log in to the Policy Editor. This account has the privilege to administer monitoring configuration.

NOTE: The `cgadmin`, `dbauser`, and `appuser` accounts use this password.

---

9 Configure the default email host using the following information:

- **SMTP Host** – The full name, including domain name, of the email server from which you want to send scheduled reports by email. You must be able to resolve the specified hostname from the Change Guardian server.
- **SMTP Port** – The remote SMTP port used to connect. The default is 25.
- **From** – The return email address appearing on each email sent.
- **SMTP User Name (Optional)** – The user name to use when connecting to the SMTP server.
- **SMTP Password (Optional)** – The password corresponding with the entered SMTP user name.

NOTE: This step is necessary if you want to email reports. You can skip this step, but if you later decide to email reports and events, you must use the Change Guardian server `configure.sh` script to update this configuration.

When the Change Guardian server installation finishes, the server starts. It might take a few minutes for all services to start after installation. Wait until the installation finishes and all services start before you log in to the server.

To access the Change Guardian Web interface, specify the following URL in your Web browser:

`https://`*IP_Address_Change_Guardian_server*`:8443`

2.3 Appliance Change Guardian Server Installation

The Change Guardian server appliance is a ready-to-run software appliance built on SUSE Studio. The appliance combines a hardened SUSE Linux Enterprise Server (SLES) operating system and the Change Guardian server software integrated update service to provide an easy and seamless user experience that allows customers to leverage existing investments. You can install the software appliance on a virtual environment or on hardware.

NOTE: The SLES operating system that you receive with the appliance is customized for the Change Guardian product and does not give you access to all the features of the operating system that you would have with your own copy of SLES.

The Change Guardian appliance image is packaged in both ISO and OVF formats that can be deployed to the following virtual environments:

- VMWare (ESX/GSX/Workstation)
- OpenXen Platform (Xen Guest desktop not supported)
- Microsoft Hyper-V

You can also install the ISO appliance image directly on hardware.

To install the Change Guardian server appliance image:

1. Download the appliance image to a local server. The OVF file name is `changeguardian_server_4.1.0.0.x86_64-0.xxxx.0.ovf.tar.gz`. The ISO file name is `change_guardian_server_4.1.0.0.x86_64-0.xxxx.0.preload.iso`.
2. (Conditional) If you are using VMWare or Xen, use the OVF template to complete the following steps:
   - **2a** Extract the appliance image to your local server. If you are extracting to a Windows server, you need a program like 7-Zip or the latest version of WinRar.

     If you are extracting to a Linux server, use the following command:

     ```
     tar -zxvf changeguardian_server-4.1.0.0-xx.x86_64.iso.tar.gz
     ```
   - **2b** For VMWare, log in to the vSphere client and deploy the OVF template. For more information, see the VMWare documentation.

     NOTE: Do not use the vSphere Web client. Instead, use the vSphere thick client.

   - **2c** For Xen, launch XenCenter and import the OVF template. For more information, see the Xen documentation.

     NOTE: Do not select **Verify OVF manifest**. Do select **Use operating system fixup**.

     ---
3. (Conditional) If you are using Microsoft Hyper-V (Hyper-V documentation) or installing direct to hardware, use the ISO image to complete the following steps:
   - **3a** Burn the ISO file to a DVD or mount the image.

     NOTE: We do not support mounting the ISO image from a network share.

   - **3b** Start or reboot your computer and check the BIOS configuration of your machine. Your BIOS should allow you to start from CD/DVD drive and change the order of the media.
   - **3c** (Conditional) If you have not mounted the image, boot the DVD.
4. Power on the appliance server.

5 Select the language and keyboard layout.

6 Read and accept the Novell SUSE End User License Agreement.

7 Read and accept the NetIQ Change Guardian End User License Agreement.

8 Specify the hostname and domain name on the Hostname and Domain Name page, and verify that the **Assign Hostname to Loopback IP** option is selected.

NOTE: Only select **Change Hostname via DHCP** if you do not have a static IP address reservation.

---

9 Set the Hardware Clock to UTC, specify the time zone of the VM, and select **Change** to configure NTP date/time synchronization.

If the time appears out of sync immediately after the installation, run the following commands to restart NTP:

- `service ntp stop`
- `service ntp start`

10 Configure the following accounts:

- appliance OS root account password
- global `admin` password
- Change Guardian server `cgadmin` password
- Deselect **Use IP Address for event routing** if you can resolve the Change Guardian server host name from all of your monitored servers.

11 Configure the default email host using the following information:

- **SMTP Host** – The full name, including domain name, of the email server from which you want to send email alerts. You must be able to resolve the specified hostname from the Change Guardian server.
- **SMTP Port** – The remote SMTP port used to connect. The default is 25.
- **From** – The return email address appearing on each email sent.
- **SMTP User Name (Optional)** – The user name to use when connecting to the SMTP server.
- **SMTP Password (Optional)** – The password corresponding with the entered SMTP user name.

2.4 Configuring Change Guardian Server

After installing the Change Guardian server, you must configure several items to ensure communication for the components.

2.4.1 Verify the Server Host Name

You have the option to install the Change Guardian Server using a static IP address or a dynamic (DHCP) IP address mapped to a host name. For the Change Guardian server to work correctly when configured to DHCP, ensure the system can return its host name correctly using the following procedure:

1 Verify the host name configuration with the following command: `cat /etc/HOSTNAME`

2 Check the server host name setting with the following command: `hostname -f`

3 Verify the DHCP configuration with the following command: `cat /etc/sysconfig/network/dhcp`

NOTE: The DHCLIENT_HOSTNAME_OPTION setting should reflect the fully qualified host name of the Change Guardian server.

4 Resolve the host name to the IP address with the following command: `nslookup` *`FULLY_QUALIFIED_HOSTNAME`*

5 Resolve the server host name from the client with the following command entered from the remote server: `nslookup` *`FULLY_QUALIFIED_CHANGEGUARDIANSERVER_HOSTNAME`*

2.4.2 Ensure the Appropriate Server Ports Are Open

Enter the following command from the Change Guardian server to verify that the appropriate ports are open:

For SLES, use:

```
iptables -I INPUT -p tcp --dport <port_number> -j ACCEPT
iptables-save
```

For RHEL, use:

```
iptables -I INPUT -p tcp --dport <port_number> -j ACCEPT
service iptables save
```

For more information, see Section 1.2, "How Change Guardian Works," on page 12.

2.4.3 Configure the Server Date and Time Synchronization

To determine the current date/time configured on the Change Guardian Server, run the following command: `date -u`

To synchronize the Change Guardian Server date/time with an external time service, configure NTP.

2.4.4 Configure Server Certificates

To configure trusted connections when authenticating to the Change Guardian Web console, you must install valid certificates on the Change Guardian Server. Use the command line tool provided on the Change Guardian server to complete the following procedure.

1 su to `novell`.

2 cd to `/opt/novell/sentinel/setup`.

3 Generate certificate signing requests using the `./ssl_certs_cg` command, and make the following selections:

- **3a** Generate certificate signing requests.
- **3b** Web Server.
- **3c** Specify a certificate signing request (`.csr`) filename.
- **3d** Have your generated `.csr` file signed by a certificate authority.

4 Copy your CA root certificate chain (`ca.crt`) and the signed certificate (`.crt`) to `/opt/novell/sentinel/setup`.

5 Import the CA root certificate chain and the Web server certificate with the following commands:

5a `./ssl_certs_cg`

5b At the menu prompt, select **Import certificate authority root certificate**.

5c Enter the CA root certificate chain file name (`ca.crt`).

5d At the menu prompt, select **Import certificate authority root certificate**.

5e At the menu prompt, select **Web Server**.

5f Enter the CA root certificate chain file name `(ca.crt)`.

6 Restart the Change Guardian server using `service sentinel restart`.

7 Import the CA root certificate change to the computer where you use the Change Guardian Web console.

2.4.5 Change Default Email Host Settings

You can change the email settings after installing Change Guardian server by using the following commands:

```
cd /opt/netiq/cg/scripts
./configure.sh udei
```

2.4.6 Verify the SHMMAX Setting

The SHMMAX setting configures the maximum size, in bytes, of a shared memory segment for PostgreSQL. Desirable values for SHMMAX start in the hundreds of megabytes to a few gigabytes.

To change the kernel SHMMAX parameter, append the following information to the `/etc/sysctl.conf file`: `# for Sentinel Postgresql kernel.shmmax=1073741824`

NOTE: By default, RHEL specifies a small value for this setting so it is important to modify it when installing to this platform.

2.5 Configuring the Change Guardian Appliance for Updates

In secured environments where the appliance must run without direct Internet access, you can configure the appliance with the Subscription Management Tool (SMT). This tool enables you to upgrade the appliance to the latest versions of Change Guardian. SMT is a package proxy system that is integrated with Novell Customer Center, which hosts appliance updates, and provides key Novell Customer Center capabilities.

For information on configuring the appliance with SMT, see "Configuring Clients to Use SMT" in the SMT documentation.

2.5.1 Register the Appliance with Novell Customer Center for Updates

You must register the Change Guardian appliance with the update channel to receive patch updates.

To register the appliance:

1 Obtain your appliance registration code or the appliance activation key.

2 Log in to the Change Guardian Web console.

3 Click the **Appliance** link to launch WebYaST.

4 Click the **Registration** link.

5 Specify the following information:

- Email ID to receive updates
- System name
- Appliance registration code

2.5.2 Configure Appliance Updates

Use one of the following methods to deliver updates to the appliance:

- Subscription Management Tool (SMT) for secure environments where the appliance must run without direct Internet access.
- Zypper for interactive updates.
- WebYaST for Web-based remote console updates.

Configure Subscription Management Tool

For secure environments where the appliance must run without direct Internet access, configure the appliance using the Subscription Management Tool.

1 Log in to the appliance console as the root user.

2 Refresh the repository for upgrade with the following command: `zypper ref -s`

3 Check whether the appliance is enabled for upgrade with the following command: `zypper lr`

4 Check the available updates for the appliance with the following command: `zypper lu`

5 Check the packages that include the available updates for the appliance with the following command: `zypper lp -r SMT-http_smt_server_fqdn:package_name`

6 Update the appliance with the following command: `zypper up -t patch -r SMT-http_smt_server_fqdn:package_name`

7 Restart the appliance.

For more information, see https://www.netiq.com/documentation/sentinel71/s71_install/data/bu4wwr7.html#bsvvcfq.

3 Installing the Change Guardian Windows Components

The topics in this chapter guide you through the planning considerations before installing the Change Guardian Windows components, including the Policy Editor and the Windows agent. If you want to install a custom configuration not identified in the sections that follow, or if you have any questions, contact NetIQ Technical Support.

3.1 Policy Editor Computer Requirements

You must install the Policy Editor on a computer running Windows XP and later.

NOTE: If you install the Policy Editor on a computer running Microsoft Windows XP (64-bit) or Windows Server 2003 (64-bit), you must install Microsoft Windows Hotfix 942589. For more information, see support.microsoft.com/kb/942589.

In addition, the Policy Editor computer must include Microsoft .NET Framework 3.5 Service Pack 1 or later or .NET Framework 4.0 Extended or later.

3.2 Installing the Policy Editor

The Policy Editor interface lets you install Change Guardian modules, configure monitoring policies, and assign monitoring policies to monitored computers.

To install the Policy Editor:

1. Log on to the computer with an administrator account.
2. Download and run the installation package, `cg_windows_agent_4_1_0_0_x86-xxxx.exe`
3. Run the installation program, `IqcgInstaller.exe`, from the Change Guardian installation kit, select **Change Guardian Console**, and follow the instructions.
4. When the installation completes, click **Finish**.

3.3 Installing the Windows Agent

Change Guardian agents allow the modules to monitor computers for change. You can choose from the following Windows agent installation options:

- Install the agent locally.
- Create the silent agent installer, which allows you create your own script to use to install the agent on the computers you want to monitor.

To install the Windows Agent:

1. Log on to the computer with an administrator account.
2. Download and run the installation package, `cg_windows_agent_4_1_0_0_x86-xxxx.exe`
3. Run the installation program, `IqcgInstaller.exe`, from the Change Guardian installation kit, select **Change Guardian Agent**, and follow the instructions.
4. When prompted, enter the following information:

Agent Settings	Enter the following information to configure the Windows agent: ◆ **Communications Port**: The default port that the agent uses to communication with the Change Guardian server is 8094. ◆ **Polling Interval**: The default time the agent waits before checking for updated monitoring policies is 10 seconds. ◆ **Platforms**: Enter the monitoring platforms that will be loaded on the agent.
Policy Repository Settings	Enter the following information to connect to the Change Guardian server Policy Repository: ◆ **Repository Computer**: Enter the fully-qualified host name or the IP address of the Change Guardian server. ◆ **Communication Port**: Enter the port used to communicate with the Policy Repository. NetIQ recommends using port 8094. ◆ **Password**: Enter the `cgadmin` password you created when you installed the Change Guardian server.

5. When the installation completes, click **Finish**.

3.4 Performing a Silent Agent Installation

When you install the Windows agent, you can choose the **Create a silent installer** option, which instructs the setup program to save the communication settings you choose during installation to an agent silent installer file (`NetIQ Change Guardian.msi`), and then save this file to the Policy Editor computer when installation completes. This option also creates a file you can use for silent upgrades of Windows agents, `Upgrade NetIQ Change Guardian.exe`.

To silently install the agent to a computer you want to monitor, copy the `NetIQ Change Guardian.msi` file from your Policy Editor computer to each computer you want to monitor. Run the file from the command line, to install the agent. You can also copy the file to a network file share and use a script to distribute and execute the file on computers you want to monitor.

3.5 Using the Change Guardian Module Manager

The Change Guardian Module Manager provides you with information about licensed modules, allows you to import module licenses to the Policy Editor, and allows you to remove module licenses from the Policy Editor. To use the Module Manager, start the Policy Editor, click **NetIQ Change Guardian**, and then select **Module Manager** in the navigation pane.

When you install Change Guardian, you install all available modules. You must import the license key for each module you want to use. To import license keys, click **Import License Key**, and then select the license key for the modules you want to use. After you import the license keys, you can use the module to create and assign policies.

4 Installing and Using the UNIX Agent and UNIX Agent Manager

This chapter provides information about installing the UNIX agent on computers you want to monitor and using UNIX Agent Manager. This chapter also provides an overview of how to manage users using UNIX Agent Manager.

To install UNIX agent, complete the following checklist:

❑	Ensure you have the necessary environment. For more information, see Section 4.1, “System Requirements,” on page 30.
❑	Install UNIX Agent Manager. See Section 4.2, “Installing UNIX Agent Manager,” on page 31.
❑	Install the agent on the computer you want to manage. ◆ For information about how to install on a local computer, see Section 4.3, “Installing the Agent on the Local Computer,” on page 32. ◆ For information about how to install using an answer file, see Section 4.4.2, “Silently Installing on the Agent Computer,” on page 33. ◆ For information about how to install, or deploy, to one or more computers from the console, see Section 4.4.1, “Deploying the UNIX Agent Using UNIX Agent Manager,” on page 32.
❑	Ensure auditing is configured on your operating system. For more information about configuring auditing, see Appendix B, “Configuring UNIX Operating System Auditing,” on page 63.
❑	Install any agent hotfixes applicable to your environment. For information about how to install patches to the console and the UNIX agent, see Section 4.5, “Applying Patches to the UNIX Agent and UNIX Agent Manager,” on page 35.
❑	Set up UNIX agent users in UNIX Agent Manager. For information about how to define users, see Section 4.7, “Managing Users in UNIX Agent Manager,” on page 36.

4.1 System Requirements

For the latest information about specific supported software versions and the availability of updates, visit the Change Guardian for UNIX Supported Products page.

The UNIX agent, when used with Change Guardian, has the following system requirements.

Item	Requirement
Operating system on agent computers	One of the following: ◆ CentOS ◆ HP-UX ◆ IBM AIX ◆ Oracle Linux ◆ Oracle Solaris ◆ Red Hat Enterprise Linux ◆ SUSE Linux Enterprise Server
Operating system on UNIX Agent Manager computers	One of the following: ◆ Red Hat Enterprise Linux ◆ SUSE Linux Enterprise Server ◆ Windows 7 (32-bit and 64-bit) ◆ Windows 8 ◆ Windows Server 2008 R2 ◆ Windows Server 2008 (32-bit and 64-bit) ◆ Windows Server 2012
Memory on UNIX agent computers	UNIX agents require the following: ◆ 128 MB RAM ◆ 512 MB swap file (virtual memory)
Memory on UNIX Agent Manager computers	512 MB
Hard disk space on UNIX agent computers	350 MB plus 400 Bytes per inode used by local file systems
Hard disk space on UNIX Agent Manager computers	1.2 GB
Default port assignments	UNIX agents use the following default ports: ◆ 2620: Communication with UNIX Agent Manager. ◆ 8094: Communication with the Change Guardian Policy Repository.
Accounts	The UNIX Remote Deployment wizard uses the `su` command to access the root account on the computer on which you want to install UNIX agents. The root password is used by the wizard only at installation and is not stored.

4.2 Installing UNIX Agent Manager

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

UNIX Agent Manager includes a server component and a console. This section guides you through installing UNIX Agent Manager components on Windows or Linux computers.

4.2.1 Installing UNIX Agent Manager on a Microsoft Windows Computer

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

To install UNIX Agent Manager on a Windows computer:

1. Log on to the Windows computer using a local administrator account.
2. Run `UAMInstaller.MSI` in the root folder of the installation kit, and begin responding to the questions in the wizard.
3. When you are given the option of communication security settings, do not restrict communication to only Federal Information Processing Standard (FIPS) encrypted algorithms. This option is not yet viable for the Change Guardian environment. If you select that option, UNIX Agent Manager cannot manage agents that work with Change Guardian.
4. Complete the automatic installer wizard. The wizard guides you through installing the UNIX Agent Manager to the folder that you specify.
5. Type and confirm a password that the UNIX Agent Manager server will use for the admin user account.

4.2.2 Installing UNIX Agent Manager on a Linux Computer

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

To install the UNIX Agent Manager on a Linux computer:

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

4.3 Installing the Agent on the Local Computer

The following procedure guides you through logging on to an agent computer and locally installing to that computer.

To install an agent on the local computer:

1. Log on to an agent computer using the root account.
2. Change directories to the product installation package, and then enter the following command to start the install script:

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

3. Proceed through the prompts.
4. When you are given the option to configure the agent for use with other products, select the option only if you run NetIQ Secure Configuration Manager, NetIQ AppManager, or NetIQ Sentinel to monitor the computer. If you will not use those products, type n instead of accepting the default response of y for those questions.
5. When you are given the option to specify the restart method, NetIQ recommends that you accept the default, rclink. For more information about restart methods, see Section 4.8, "Restart Methods for the UNIX Agent," on page 37.

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

4.4 Installing the UNIX Agent

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

4.4.1 Deploying the UNIX Agent Using UNIX Agent Manager

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

- Your site standards prohibit your access to root passwords.
- Your site standards require a specific software distribution mechanism.
- Your site standards prohibit software distribution mechanisms.
- Your UNIX Agent Manager installation does not include the necessary deployment packages.

For information about installing UNIX Agent Manager, see Section 4.2, "Installing UNIX Agent Manager," on page 31.

To remotely deploy UNIX agent components:

1. In the **File** menu of UNIX Agent Manager, select **Remote Deployment**.
2. Click the **Add Host** button and fill in the fields as prompted.
3. When you are given the option of communication security settings, do not restrict communication to only Federal Information Processing Standard (FIPS) encrypted algorithms. This option is not yet viable for the Change Guardian environment. If you select that option, UNIX Agent Manager cannot manage agents that work with Change Guardian.

4 When you are given the option to specify the restart method, NetIQ recommends that you accept the default, rclink. For more information about restart methods, see Section 4.8, "Restart Methods for the UNIX Agent," on page 37.

5 Proceed through the wizard to complete installation.

4.4.2 Silently Installing on the Agent Computer

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

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

Parameter	Description
`FRESH_INSTALL`	Specifies whether you want the install program to install the agent only as defined in the silent install file, or if you want to use the installation to add product support to an existing agent. Valid entries are `1`, to install the agent normally and `0`, to add an additional product to an existing agent installation. The default is `1`.
`CREATE_TARGET_DIR`	Specifies whether you want the install program to create the target installation directory if it does not already exist. Valid entries are `y` and `n`. The default is `y`.
`CONTINUE_WITHOUT_PATCHES`	Specifies whether the install program stops or continues when the operating system is not a supported version. Valid entries are `y` and `n`. The default is `n`.
`IQCONNECT_PORT`	Specifies the port that the UNIX agent uses to communicate with UNIX Agent Manager. The default is `2620`.
`IQ_STARTUP`	Specifies restart method for the uagent process. This process is used by the UNIX agent for the Change Guardian, AppManager, Sentinel, and Secure Configuration Manager products. For information about the options, see Section 4.8, "Restart Methods for the UNIX Agent," on page 37. Valid entries are `rclink` and `inittab`. The default is `rclink`.

Parameter	Description
USE_FIPS_COMMON	Specifies whether the UNIX agent communicates with UNIX Agent Manager using only Federal Information Processing Standard (FIPS) encrypted algorithms. Ensure this is set to 0. This option is not yet viable for the Change Guardian environment. If you select that option, UNIX Agent Manager cannot manage agents that work with Change Guardian.
INSTALL_CGU	Specifies whether the UNIX 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 UNIX agent will use to communicate with the Change Guardian Policy Repository. The default is 8094.
IQRM_USER	Specifies the account that the UNIX agent uses when accessing the Change Guardian Policy Repository.
IQRM_PASS	Specifies the password for the account that the UNIX agent uses when accessing the Change Guardian Policy Repository.
IQCONFIG_RECONNECT	Specifies how often, in minutes, the UNIX agent checks for new information in the Change Guardian Policy Repository. For example, 2.
CGU_STARTUP	Specifies restart method for the detectd process. For information about the options, see Section 4.8, "Restart Methods for the UNIX Agent," on page 37. Valid entries are rclink and inittab. The default is rclink.
MANAGE_AUDIT_LOGS	Specifies whether the UNIX agent reduces the size and removed old audit logs. Valid entries are y and n.
AUDIT_LOG_SIZE	Specifies the maximum size, in bytes, that the UNIX agent allows an audit log to reach before starting a new log.
AUDIT_LOG_RETENTION	Specifies the number of audit logs that the UNIX 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 from version 7.1 of the UNIX agent. Valid entries are y and n.
OLD_INSTALL_DIR_MOVED	Specifies the directory where you want the installation program to move the previous installation directory.

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

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

Where <Target_Directory> is the directory you want to install to and <SilentConfigurationFile> is the file name you used to specify the installation options. You can also use the default configuration file, `SampleSilentInstallation.cfg`.

The script will then extract information from the installation file and install the agent according to the values you have specified.

NOTE: The installation filename must be specified as an absolute path. By default, `SampleSilentInstallation.cfg` is located in the UNIX agent install directory.

4.5 Applying Patches to the UNIX Agent and UNIX Agent Manager

NetIQ provides patches in a zipped file known as a **p-ball** for agent components and in a zipped file with the extension `.um` for UNIX Agent Manager.

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

4.6 Uninstalling UNIX Agents and UNIX Agent Manager

You can uninstall the UNIX agent components manually or using UNIX Agent Manager.

4.6.1 Uninstalling the UNIX Agent

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

NOTE: You do not need to uninstall agents with a lower version number before upgrading agents. Use this procedure only if you want to completely remove agents from remote computers. For more information about upgrading agents, see Section 4.9, “Saving UNIX Agent Information to a File,” on page 38.

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

```
./uninstall.sh
```

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

4.6.2 Uninstalling UNIX Agent Manager

To uninstall the UNIX Agent Manager on Windows computers, use the **Add/Remove Programs** Control Panel to remove the **UNIX Agent Manager** program. If you had previous versions of the UNIX Agent Manager installed, also ensure that all files and directories are removed.

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

4.7 Managing Users in UNIX Agent Manager

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

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

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

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

4.7.1 Using LDAP or Microsoft Active Directory Credentials

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

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

1. Ensure you have the following information:
   - The domain and computer address, such as ldap://houston.itservice.production:389, of the LDAP or Active Directory server
   - The location of the user entries in the structure of the LDAP or Active Directory server
   - The attribute that identifies the login name for each user
   - An account that UNIX Agent Manager server can use to access the LDAP or Active Directory server
2. Log into a UNIX Agent Manager console as an administrator, and open the **Manage Server** window.
3. Click the **LDAP** tab, then the **Add** button.
4. Enter the name of the domain that contains the LDAP or AD server. Users must also enter this domain name when they log into UNIX Agent Manager.

5. Select the domain and provide the information as requested on the window using the following guidelines:
   - In **Server Address**, enter LDAP or Active Directory server computer name and port. For example, `ldap://houston.itservice.production:389`
   - In **User's Parent DN**, enter the path to the node that contains the usernames you want to use. For example, `ou=AMAdmins,dc=netiq,dn=com`
   - In **Username Attribute**, enter the attribute you want UNIX Agent Manager to use to identify the user. This attribute will be used as a consistent identifier even if the user name changes. The default and only attribute supported by UNIX Agent Manager 7.2 is `uid`
   - (Conditional) If you use simple authentication for specific users, in **Username**, enter the path to the user name. For example, `ou=Operator,dc=netiq,dn=com`
6. Click **Refresh Users**.
7.

4.7.2 SSL Communication with the LDAP or Active Directory Server

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

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

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

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

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

4.8 Restart Methods for the UNIX Agent

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

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

4.9 Saving UNIX Agent Information to a File

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

5 Setting Up Your Environment for Monitoring

This chapter guides you through using the Change Guardian Policy Editor, including assigning policies, creating policy sets, setting group membership, and creating reports.

5.1 Logging into Change Guardian

The Policy Editor allows you to submit and assign policies and policy sets to the computers and asset groups in your enterprise.When you start the Policy Editor you connect to the Policy Repository, which runs on the Change Guardian server, with an account that is a member of the admin or CG Admin group. You can omit this step in the future by selecting `Auto login`.

5.2 Creating Policies and Policy Sets

Change Guardian **policies** allow you to define how Change Guardian monitors assets in your environment. Each Change Guardian module includes several policy types for the respective platforms they support. Policy sets allow you to group policies together to organize and to assign monitoring.

You can create a new policy by cloning an out-of-the-box template or navigating to the policy type you want to monitor (such as Active Directory Policies > AD Object), and clicking `Create Policy`.

5.2.1 Understanding Policies

A policy includes one or more constraints to define a specific change event you want to monitor in your enterprise.

Policies allow you to identify the monitoring target, and then add any combination of the following constraints:

- Add filters to more precisely narrow the monitoring target and results
- Define managed users for the activity
- Define custom event severities
- Assign event contexts to categorize policies
- Specify event severity generated for events matching this policy

Designating Managed Users

Change Guardian allows you to designate specific users to make specific changes. These users are managed users. Events generated when managed users make changes appear as managed change events. Users who are not authorized to make changes are unmanaged users.

When **Severity** is set to `Auto`, the severity is calculated based on wether the user is authorized and if the action was successful. For example:

- Sev 5 - unauthorized & success
- Sev 4 - unauthorized & fail
- Sev 3 - authorized & fail
- Sev 2- authorized & success
- Sev 0&1 - system events

You can customize the severity in the policy definition.

The **Events are considered managed for** pane allows you to specify one or more users as managed users authorized to perform the action on the asset the policy monitors.

You can also specify user groups as managed users. As group membership changes, Change Guardian synchronizes policies with the new group members. For more information, see Section 5.3, "Understanding Resource Expansion," on page 43.

Understanding Event Context

You can use **event context**, such as risk, vulnerability, or regulation, to categorize a policy and specify the purpose of the policy to other members of your enterprise. Events generated by these policies include the event contexts. You can select from a list of default event context options or create additional contexts.

Risk Domain

Categorize the risk domain of the event:

- operational continuity
- financial viability
- reputation and good will
- civil
- criminal
- environmental
- intangible
- information security
- information integrity

Risk

Categorize event risk as high, medium, low, informational.

Sensitivity

Categorize event sensitivity level as Public, Internal, Restricted, Confidential, or Secret.

Regulation/Policy

You can classify monitoring policies as compliant with regulations such as Sarbanes-Oxley, PCI-DSS, FDA Part 11, GLBA, FISMA, HIPAA, COBIT, NIST, AS 3806, APRA, and C-SOX.

Control/Classification

User-defined String

Response Window

User-defined String

Submitting a Policy

When you use a Change Guardian module to create and modify a policy, you can save your changes in one of the following states:

Submitted

Policy saved as a new revision to the Policy Repository. The Change Guardian sever stores all policy revisions, which are accessible to any user logged into a Policy Editor. You enable one policy revision, which is sent to assigned assets.

Enabled

Policy saved as a new revision to the Policy Repository. Other users can access the policy. This option also enables the policy revision, which makes the saved revision of the policy available for assignment. If you modified a policy revision already assigned to computers, this option updates that policy to all computers with the policy assigned. When you update the enabled revision of a policy, monitored assets that have that policy assigned are automatically updated with the new revision.

You cannot enable or assign policies, or make policies available to others, until you submit policies to the Policy Repository.

Enabling a Policy Revision

When you submit a policy to the Policy Repository, you must enable the policy before you can assign it to monitor computers or asset groups. You can choose whether to enable the policy immediately, or choose to submit the policy without enabling it. Later, you can enable the policy from the selected module window.

To enable a policy revision from a Change Guardian module window:

1. In the left pane, select the policy.
2. Select the **History** tab.
3. Select the version of the policy you want to enable.
4. Click **Enable**.

Loading a Policy Revision

When you make changes to a policy and then submit that policy, Change Guardian creates a new revision of that policy in the Policy Repository. You can view all revisions of a policy stored in the Policy Repository. Policy revisions allow you to keep and share works in progress, and you can choose to load a previous revision of the policy to edit or enable. The properties section displays the version number of the currently loaded policy, and the state of the enabled policy.

The History tab indicates the enabled policy version by displaying a check mark in the **Enabled** column of the lower table.

Exporting and Importing a Policy Revision

Change Guardian allows you to export a policy to an `.xml` file. You can import a valid policy that was previously exported for future use as a new policy. You can modify an imported policy to easily create a new policy with a similar definition.

You can export one policy at a time but import multiple policies at a time.

Cloning a Policy

Cloning a policy allows you to quickly create a new policy based on a selected existing policy, and then make changes as needed. By default Change Guardian uses the loaded version of the selected policy when creating a clone, but you can select a specific policy version.

5.2.2 Using Out-of-the-box Policy Templates

Change Guardian out-of-the-box policy templates provide examples of policies and best practice content you can reuse. Applying a policy template from the platform template library will clone the policy into your active policy area. When a copy of the template appears in the list of policies for the module, you can edit the constraints to specify your monitored computers and files.

5.2.3 Understanding Policy Sets

The Policy Set Manager allows you to combine multiple policies from one or more Change Guardian modules to form policy sets. Policy sets allow you to organize and manage monitoring needs for a specific use case. Also, reusing policies in multiple policy sets cuts down on the total number of policies needed in the system.

If you apply a policy to a group that contains multiple asset types, such as Windows and UNIX, the policy applies only on the asset that is applicable. For example, if you apply a UNIX policy to a group that contains Windows and UNIX assets, the policy applies to the UNIX assets only.

To view policy sets, click **NetIQ Change Guardian**, and then select **Policy Set Manager** in the left pane.

Adding and Editing a Policy Set

The Policy Set Manager allows you to add any submitted policy from any Change Guardian module to a policy set.

Click **Policy Set Manager** to view policy sets you created and to add new policy sets. Select a specific policy set to delete, clone, or edit its details. After you create a policy set, you can assign the set as you would assign a policy. For more information, see Section 5.5, "Assigning Policies and Policy Sets," on page 45.

Cloning a Policy Set

Cloning a policy set allows you to quickly create a new policy set based on a selected existing policy set, and then make needed changes.

5.3 Understanding Resource Expansion

Change Guardian uses resource expansion to process each user group specified in a policy as a list of the group members. For example, if a policy specifies a user group to monitor, Change Guardian uses the resource expansion configuration to monitor for activity performed by the individual users in the group. If the policy returns an event, the name of the user performing the change appears in the event report.

NOTE: You must configure resource expansion for every grouped resource. If you do not configure resource expansion for a grouped resource and you specify that grouped resource in a policy, the Policy Editor cannot submit the policy to the Change Guardian Server.

To access resource expansion, click **Settings > Resource Expansion**.

The Resource Expansion Configuration window lists the **scope**, or domain name, for each expanded resource. From this window, you can choose to expand a new resource or edit an existing expanded resource.

Creating or editing an expanded resource requires you to define the **resource type**, which includes the domain, type of resource, and the credentials to allow access to group information.

5.4 Understanding and Managing Asset Groups

You can place computers in **asset groups** to categorize them, or assign policies to many computers with one policy assignment. Dynamic group membership is updated every 30 minutes. Default groups have a constraint to match specific platforms and cannot be deleted. Static groups require manual updates to change the members of the group.

Asset Membership displays your asset groups and the monitored computers each asset group contains. You can centralize administration of your monitored computers by creating asset groups, and applying policies or policy sets to monitor multiple computers that require the same level of monitoring. Rather than assign policies separately to multiple computers, you can place those computers in an asset group, and then assign policies only once to the asset group. Policies assigned to an asset group are automatically deployed to a monitored target when it joins the group.

Click **NetIQ Change Guardian**, and then select Asset Groups to perform the following functions:

- Add and remove asset groups

- Add and remove computers to and from asset groups
- Edit computers in asset groups
- View computers in your enterprise, and the asset groups to which a selected computer belongs
- View computer attributes, such as computer name and operating system
- View asset groups, and the computers each group contains

Select **Computers** to see a list of computers with Change Guardian agents installed. Select **Asset Groups** to see a list of asset groups and the computers they contain.

5.4.1 Filtering Assets and Asset Groups

If Change Guardian lists a large number of assets and asset groups, you can use **Filter Values** to expand the pane, and then use any of the following conditions to narrow the view of assets or asset groups:

Contains

Enter a string of characters that appears anywhere within the names of assets or asset groups you wish to view into the **Set value** text box.

Does not contain

Enter a string of characters that does not appear within the names of assets or asset groups you wish to view into the **Set value** text box.

Starts with

Enter the first characters of the asset or asset group names you wish to view into the **Set value** text box.

Ends with

Enter the last characters of the asset or asset group names you wish to view into the **Set value** text box.

Equals

Enter the name of the asset or asset group to which you want to apply a policy or policy set into the **Set value** text box.

Does not equal

Exclude a asset or asset group from the list by entering the asset or asset group name into the **Set value** text box.

Matches

Enter a name, or a partial name and wildcard, of the asset or asset group to which you want to apply a policy or policy set into the **Set value** text box.

After you select a condition and enter a value for the filter, click **Apply** to display a list of computers or asset groups matching the filter you created. Filter values are cumulative, so you can further narrow the list of computers or asset groups by adding conditions and values to your filters.

5.4.2 Editing Computers in Your Asset Groups

To view a list of computers in an asset group, select an asset group, and then select the Membership tab. From the Membership tab, you can add, edit, or remove computers to the asset group.

5.4.3 Viewing Computers in Your Enterprise

The Asset Groups node can display information about the monitored computers in your enterprise. Select **Assets** to view monitored computers.

From the **Attributes** tab you can view information about a selected computer.

From the **Membership** tab, you can view the groups to which the selected computer belongs, add the computer to other groups, and remove the computer from asset groups.

TIP: If you have a long list of monitored computers, use the **Filter Values** feature to display only those computers matching a specified naming pattern.

5.5 Assigning Policies and Policy Sets

After you create a policy, it is stored in the Change Guardian Policy Repository, which makes the policy available to other Change Guardian users in your enterprise, and enables the policy for assignment to computers and asset groups.

The Policy Assignment screen allows you to assign policies and policy sets to the assets or asset groups in your enterprise, or the asset groups you created. Selecting an asset or asset group allows you to see the policies and policy sets assigned to it, and allows you assign additional policies and policy sets.

5.6 Creating Monitoring Schedules

You can create and configure monitoring schedules that are available as part of assigning policies or policy sets. By default, Change Guardian policies monitor computers and asset groups continuously. Scheduled monitoring allows you to specify that an assigned policy or policy set monitors computers and asset groups during specific time frames. For example, you can suspend monitoring during maintenance windows for computers or asset groups, which eliminates events generated as a result of the maintenance.

Scheduled monitoring supports days of the week and inclusive intervals during a day.

Examples of valid time restrictions include the following:

- Mondays, Tuesdays, and Wednesdays from 3-5 PM
- Mondays from 3-5 PM and Tuesdays from 4-6 PM
- Mondays from Midnight-7 AM, 9 AM-2 PM, and 6 PM-Midnight

To create a monitoring schedule:

1. Log in to the Change Guardian Policy Editor.
2. Click **Settings > Schedule Monitoring Time**.
3. Click **Add**.
4. In the **Schedule Name** field, type a name for the schedule.
5. In the **Schedule Monitoring Time** window, select the time and day you want Change Guardian to stop monitoring, and then select **Don't Monitor**.

TIP: You can drag your cursor to select a range of times and days for scheduled monitoring.

6. Click **OK**.

To edit an existing monitoring schedule:

1. Log in to the Change Guardian Policy Editor.
2. Click **Settings > Schedule Monitoring Time**.
3. Select an existing schedule name.
4. Click **Edit**.
5. Make the desired changes to the monitoring schedule.
6. Click **OK**.

5.7 Understanding Change Guardian Email Alerts

You can configure Change Guardian to send email notifications for events to specified administrators and operators. **Email Configuration** in the Policy Editor defines the SMTP connection information and email format settings for actions that are exposed through Routing in the Change Guardian Web console. Once configured, you can define a routing rule to send an email for incoming events that match a specified Lucene filter.

Event Routing in the Change Guardian Web console uses the information supplied in the email integrators to assign email alerts to specified events. For more information, see Section 6.8, "Assigning Email Alerts to Events," on page 51.

5.7.1 Creating and Configuring Email Server

To enable email alerts, you must create an email server and store it on an event destination computer. If your Change Guardian environment includes more than one event destination computer, you must create an email integrator on each event destination from which you want to send email alerts.

To create and configure an email integrator:

1. **Select Settings > Email Configuration**.
2. Under the Email Servers pane, click **Add**.
3. Type the name of the email server you want to use to send email.
4. Type a description for the email server.
5. Enter values for the following fields:
   - SMTP Host – The full name, including domain name, of the email server from which you want to send email alerts.
   - SMTP Port – The remote SMTP port to which the integrator connects.
   - Secure – Specifies if the connection to the SMTP computer must be a secure connection.
   - From – The return email address appearing on each email alert for this email integrator.
   - Authentication Required – Specifies if the email server requires SMPT authentication to send email.
   - User Name – The user name to use when connecting to the SMTP server.
   - Password – The password corresponding with the entered SMTP user name.

5.7.2 Creating and Configuring Notification Groups

As part of creating an email server, you must create one or more notification groups, which specify the recipients of the email alerts and contains change event information. When you assign email alerts to events in the Change Guardian Web console, you can choose from all notification groups available for that event destination. For more information, see Section 6.8, "Assigning Email Alerts to Events," on page 51.

NOTE: If you want only one person to receive an email alert, you must create a notification group containing only the desired email address.

To create and configure a notification group:

1. **Select Settings > Email Configuration**.
2. Specify an email server.
3. Under the Notification Groups pane, click **Add**.
4. Type the name of the notification group you want to create.
5. Type a description for the notification group.
6. Enter values for the following fields:
   - From – The return email address appearing on each email alert for this email integrator.
   - To – A list of email addresses, separated by commas, that receive email alerts.
   - CC – A list of email addresses, separated by commas, that receive copies of email alerts.
   - BCC – A list of email addresses, separated by commas, that receive blind copies of email alerts.
   - Subject – The subject appearing on the alert email.
   - Max Events per Email – Specifies the number of events displayed in the email alert. The email includes the events received up to the maximum number set in this field.
   - Include Change Details – Specifies whether the body of the email contains the details of the change detected by Change Guardian.
   - Email Format – Specifies the format of the email as either text or HTML.

5.8 Using Change Guardian Administrative Reports

Change Guardian allows you to create customized reports detailing the Change Guardian configuration for your enterprise. Administrative reports can contain information such as the computers in each asset group and a list of the current policy assignments by asset group. You can use this information for auditing or administration purposes.

You can save the generated report as a PDF file. You can also use the Policy Editor to print reports, or send reports to others as an email attachment.

Change Guardian generates the following reports:

Assigned Policies by Asset

This report returns a list of assigned policies for each asset or asset group specified in the report conditions. If you choose to show details, the report includes a subsection with the definition of each assigned policy. This report includes the following report conditions:

- Show policies assigned to specified assets
- Show policies assigned to assets in specified asset groups

- Show policies assigned to specified asset groups
- Show or hide policy assignment details
- Show event destination assigned to policies assigned to specified assets
- Show monitoring schedules assigned to policies assigned to specified assets

Assets by Assigned Policy

This report returns a list of assets assigned for the policies or policy sets specified in the report conditions. This report includes the following report conditions:

- Show assets assigned to specified policies
- Show assets assigned to policies in specified policy sets

Policies Not Assigned

This report returns the list of policies defined, but not assigned to an asset.

Managed Assets

This report returns a list of registered assets, sorted either by asset name or by asset registration.

Asset Monitor Failures

This report returns a list of policy assignment failures showing the following information: Impact, Error Code, Issue and the failure date.

6 Viewing Change Guardian Events

This chapter describes using the Change Guardian Web console to view events. Change Guardian displays events—results from assigned policies and policy sets—through event reports displayed in the Change Guardian Web console. To access the Web console, specify the following Web address, as determined by your Change Guardian sever installation:

`https://`*`Change_Guardian_Server_IP_Address`*`:8443`

When prompted, enter your Change Guardian user name and password.

6.1 Supported Web Browsers and Settings

You can view Change Guardian event reports from a Windows or Linux computer with one of the following Web browsers installed:

- Microsoft Internet Explorer 8 or later
- Mozilla Firefox 5 or later

To view event reports in Internet Explorer 8, ensure the following:

- Set the security level to Medium-high. If you set the security level to High, the Web console displays a blank page. On the **Tools** menu, select **Internet Options > Security**, and then set the security level to Medium-high.
- Ensure you do not select the **Compatibility View** option on the **Tools** menu.
- Enable automatic prompting for file downloads to ensure a pop-up blocker does not prevent the file download. On the **Tools** menu, select **Internet Options > Security > Custom Level**, scroll down to **Downloads**, and then select **Enable** as the **Automatic prompting for file downloads** option.

6.2 Understanding Event Information

The Change Guardian Web console, by default, displays events with a severity of 0 to a severity of 5. Using the default filter, you can view the following information for each event:

- The specific alert severity
- The name of the file changed or accessed, or the name of the Active Directory object changed
- The computer on which that file resides or the domain controller computer on which the active directory change occurred
- Delta information (detected difference in the monitored file or active directory object), when applicable
- Differential (diff) information (the actual changes made to the monitored file)

NOTE: Events reflecting changes to binary files include only delta information. These events do not include diff information.

6.3 Viewing Detailed Event Information

The Change Guardian Web console allows you to schedule reports and see additional detail for each event. This section describes the configuration options for customizing the information you see for each event.

To see detailed event information, click the shield icon.

6.4 Reports

The Change Guardian Web console includes a report for policy events. When you run the report, you can choose to use default options or to customize any of the following options:

- The frequency you want to run the report
- A saved name for the report
- A date range for events
- A specific event type
- A specific policy
- View all events, managed events only or unmanaged events only
- View all change events, only successful change attempts, or only failed change attempts
- View events of a specified severity range
- Choose to send the report to a specified email address

6.5 People

You can use Change Guardian with NetIQ Identity Manager, which allows you to view the user identity details of events. You must have the View People Browser permission to view the identity details.

To view the user identity details of an event:

1. Perform a search, and refine the search results as needed.
2. In the search results, select the events for which you want to view the identity details.
3. Click ***Event operations > Show identity details***.
4. Select whether you want to view the identity of the Initiator user, the Target user, or both.

If you do not have Identity Manager or a similar product installed, this option is not available. For more information about integrating identity information with Change Guardian events, see Integrating Identity Information with Sentinel Events in the *NetIQ Sentinel User Guide*.

6.6 Tags

Tags are user-defined values you can use to logically group data collection objects such as event sources, event source servers, report templates, and report results. For example, you can create tags such as “PCI” and “HR” to help you group information.

Tags help you to filter object lists for the data collection objects and also to augment incoming data. You can search for events, report templates, and report definitions that are tagged with a particular tag.

6.7 Filters

Filters allow you to customize event searches and prevent data overload. The Filter Builder helps you build search queries ranging from simple to complex. You can save a search query as a filter and reuse it as required to quickly perform a search by selecting the filter rather than specifying the query manually every time.

For more information about filters, see Configuring Filters in the *NetIQ Sentinel User Guide*.

6.8 Assigning Email Alerts to Events

To send email messages from within the Change Guardian Web console, you must create an event routing rule, and you must have an email integrator configured for the Web console computer. If you do not have an email integrator configured, no notification groups appear as available actions for the event routing rule. For more information on configuring email integrators, see Section 5.7, “Understanding Change Guardian Email Alerts,” on page 46.

To assign email alerts to an event:

1. Start the Change Guardian Web console.
2. Click **Routing**.
3. Click **Create**.
4. Enter the following event routing information:
   - Name – The name for the event routing rule.
   - Filter – A filter to match the Change Guardian event, severity, or both for which you want to send email alerts.
   - Tag – An optional field to provide additional filtering.
   - Action – Available notification groups.
5. Click **OK**.

NOTE: You can assign more than one email alert to a specific event by assigning more than one action to the event routing rule

---

6.9 Forwarding Events for Long-Term Retention

Change Guardian stores raw data and compressed event data on the local file system. You can configure Sentinel to store the data in a networked location for long-term storage.

The data files are deleted from the local and networked storage locations on a configured schedule. Raw data retention is governed by a single raw data retention policy. Data retention is governed by a set of event data retention policies. All of these policies are configured by the Change Guardian administrator. By default, Change Guardian retains event data for 30 days.

Change Guardian uses the same data storage and retention policy technology as NetIQ Sentinel. For more information, see Configuring Data Storage in the *Sentinel Administration Guide*.

7 Upgrading Change Guardian

This chapter addresses planning considerations and provides a checklist to help you upgrade to the most current version of Change Guardian. The upgrade process does not support upgrading from versions of Change Guardian prior to version 4.0. If for any reason you need to uninstall Change Guardian, contact Technical Support prior to uninstalling the product.

7.1 Change Guardian Upgrade Checklist

Upgrade your Change Guardian installation using the following checklist. You must upgrade both the Change Guardian server and the Policy Editor. The Windows and UNIX agents are backwards compatible.

Table 7-1 *Upgrade Checklist*

❒	Tasks	See
❒	Ensure that the computers on which you install Change Guardian and its components meet the specified requirements.	Supported Platforms on the NetIQ web site
❒	Review the supported operating system release notes to understand the known issues.	SUSE Release Notes
❒	Review the Change Guardian release notes to see new functionality and understand the known issues.	Change Guardian Release Notes
❒	Upgrade the Change Guardian server.	Section 7.2, “Upgrading the Change Guardian Server,” on page 53
❒	Upgrade the Policy Editor.	Section 7.3, “Upgrading Windows-Based Components,” on page 55
❒	(Optional) Upgrade the Windows Agent.	Section 7.3, “Upgrading Windows-Based Components,” on page 55

7.2 Upgrading the Change Guardian Server

Upgrade the Change Guardian server on either an existing Linux server (traditional installation) or as a managed software appliance (appliance installation).

7.2.1 Upgrading a Traditional Installation

IMPORTANT: Change Guardian requires that the operating system must be IPv6 enabled. Ensure that IPv6 is enabled in the operating system before you upgrade your system. If IPv6 is not enabled, major components will fail to operate.

To upgrade the Change Guardian server running a traditional installation:

1. Back up your configuration and event information using the `backup_util.sh` script. For information about using the backup utility, see Backing Up and Restoring Data (https://www.netiq.com/documentation/sentinel71/s71_admin/data/bn1fcap.html).
2. Download the latest installer from the NetIQ download Web site. You must be a registered user to download patches. If you have not registered, click **Register** to create a user account in the patch download site.
3. Log in as `root` to the server where you want to upgrade Change Guardian.
4. Specify the following command to extract the install files from the tar file:

   `tar -zxvf <install_filename>`

   where <*install_filename*> is the name of the install file.
5. Change to the directory where the install file was extracted.
6. Specify the following command to upgrade Change Guardian:

   `./install-changeguardian.sh`
7. To proceed with a language of your choice, select the number next to the language.
8. (Conditional) If there are changes to the end user license agreement, read and accept the changes.
9. Specify `yes` to approve the upgrade
10. Reset the cgadmin password to leverage LDAP authentication.
11. Verify the Change Guardian Web console can connect to the server by specifying the following URL in your Web browser:

`https://IP_Address_Change_Guardian_server:8443`

7.2.2 Upgrading an Appliance Installation

To upgrade the Change Guardian server running as a managed software appliance, you can use Zypper (a command line package manager) or WebYaST (a web-based remote console). For information, see Using Zypper and Using WebYaST.

In some instances, such as an end user license agreement update, you must upgrade the Change Guardian server appliance using Zypper. For information on which methods of upgrade are supported for a release, see the Release Notes (https://www.netiq.com/documentation/change-guardian/).

To upgrade the appliance using Zypper, perform the following steps:

1. Back up your configuration and event information using the `backup_util.sh` script. For information about using the backup utility, see Backing Up and Restoring Data (https://www.netiq.com/documentation/sentinel71/s71_admin/data/bn1fcap.html).
2. Log in to the appliance console as the `root` user

3 To check for available updates, run the command `zypper lp`.

4 Install the updates by running the command `/usr/bin/zypper patch`.

5 Restart the Change Guardian appliance by running the command `reboot`.

To upgrade the appliance using WebYaST, perform the following steps:

1 Log in to the Change Guardian appliance as a user in the administrator role.

2 Click **Appliance** to launch WebYaST.

3 Back up your configuration and event information using the `backup_util.sh` script. For information about using the backup utility, see Backing Up and Restoring Data (https://www.netiq.com/documentation/sentinel71/s71_admin/data/bn1fcap.html).

4 (Conditional) If you have not already registered the appliance for automatic updates, register for updates. For more information, see Register the Appliance for Updates.

If the appliance is not registered, Change Guardian displays a yellow warning that indicates that the appliance is not registered.

5 To check if there are any updates, click *Updates*.

6 Select and apply the updates.

Before upgrading the appliance, WebYaST automatically stops the Change Guardian service. You must manually restart this service after the upgrade is complete. The updates might take a few minutes to complete.

7 Restart the Change Guardian service.

Using Zypper

Use Zypper to perform interactive updates on the appliance.

1 Log in to the appliance as root.

2 Run the following command: `/usr/bin/zypper patch`

3 Restart the appliance.

For more information, see the Zypper Cheat Sheet.

Using WebYaST

Use WebYaST to manage appliance updates from a Web-based remote console. You can access WebYast through the Change Guardian Web console appliance dialog. You can also access WebYast directly at (https://IP_Address_Change_Guardian_Server:54984).

For more information, see the WebYaST documentation.

7.3 Upgrading Windows-Based Components

You can use the `IqcgInstaller.exe` program in the installation kit to locally upgrade the Policy Editor or Windows agent or create a silent installer package for upgrading multiple agents.

To upgrade Windows-based components:

1 Download the latest installer from the NetIQ download Web site. You must be a registered user to download patches. If you have not registered, click Register to create a user account in the patch download site.

2 Double-click the download image and extract the installation media.

3 To upgrade the locally installed Windows components, run the Windows installer. The program upgrades previously deployed components.

4 (Optional) To distribute the Windows agent to multiple computers, complete the following steps for creating a silent installer package.

   4a Run the `IqcgInstaller.exe` program and follow the steps until you get to the Change Guardian Agent window.

   4b In the Change Guardian Agent window, clear **Install the selected components locally**.

   4c Select **Create a silent installer**.

   4d Specify the location for the silent installer package.

   4e The setup program creates a silent installer package called `Upgrade NetIQ Change Guardian.exe`. Run this program to upgrade your remote agents.

   NOTE: When you specify **Create a silent installer**, the setup program also creates `NetIQ Change Guardian.msi` file in the specified path. To use this program to upgrade your agents, you must use the following command to run the file: `msiexec.exe /i "NetIQ Change Guardian.msi" REINSTALL=ALL REINSTALLMODE=vomus`.

A Configuring Your Active Directory Environment

After you install Change Guardian you must configure your Active Directory environment to ensure that the operating system generates and retains Active Directory events until Change Guardian processes them. The following items must be configured by someone with domain administrator permissions for the Windows domains that Change Guardian monitors:

- Security event log
- Active Directory auditing
- Active Directory security access control lists (SACLs)

A.1 Configuring the Security Event Log

You must configure the security event log to ensure that Active Directory events remain in the event log until Change Guardian processes them.

Set the maximum size of the Security Event Log to no less than 10 MB, and set the retention method to **Overwrite events as needed**.

To configure the security event log:

1. Log on to a computer in the domain you want to configure using a user account with domain administrator privileges.
2. Open a command prompt, type `gpmc.msc` and press **Enter** to start the Group Policy Management Console.
3. Expand **Forest > Domains >** ***domainName*** **> Domain Controllers**.
4. Right-click **Default Domain Controllers Policy**, and then click **Edit**.

   NOTE: Making this change to the default domain controllers policy is important because a GPO linked to the domain controller (DC) organizational unit (OU) with a higher link order can override this configuration when you restart the computer or run `gpUpdate` again. If your corporate standards do not allow you to modify the default domain controllers policy, create a GPO for your Change Guardian settings, add these settings to the GPO, and set it to have the highest link order in the Domain Controllers OU.
5. Expand **Computer configuration > Policies > Windows Settings > Security Settings**.
6. Select **Event Log** and configure **Maximum security log size** to a size of no less than 10240 KB (10 MB).
7. Configure **Retention method for security log** to **Overwrite events as needed**.
8. Return to the command prompt, type `gpUpdate` and press **Enter**.

To verify this configuration and ensure Active Directory events are not discarded before processing:

1. Open a command prompt as an administrator.
2. At the command line, type `eventvwr` to start the Event Viewer.
3. In Windows logs, right-click **Security**, and select **Properties**.
4. Verify the settings reflect a maximum log size of no less than 10240 KB (10 MB), and the selection to **Overwrite events as needed**.

A.2 Configuring Active Directory Auditing

This configuration enables auditing of Active Directory events and logs the events in the security event log.

You should configure the Default Domain Controllers Policy GPO with Audit Directory Service Access set to monitor both success and failure events.

To verify or set this configuration:

1. Log on to a computer in the domain you want to configure using a user account with domain administrator privileges.
2. Open a command prompt, type `gpmc.msc` and press **Enter** to start the Group Policy Management Console.
3. Expand **Forest > Domains >** ***domainName*** **> Domain Controllers**.
4. Right-click **Default Domain Controllers Policy**, and then click **Edit**.

   NOTE: Making this change to the default domain controllers policy is important because a GPO linked to the domain controller (DC) organizational unit (OU) with a higher link order can override this configuration when you restart the computer or run `gpUpdate` again. If your corporate standards do not allow you to modify the default domain controllers policy, create a GPO for your Change Guardian settings, add these settings to the GPO, and set it to have the highest link order in the Domain Controllers OU.

5. Expand **Computer configuration > Policies > Windows Settings > Security Settings**.
6. (Conditional) For Windows Server 2008 R2 and later, complete the following steps:
   - **6a** In **Security Settings**, expand **Advanced Audit Policy Configuration > Audit Policies**.
   - **6b** For CGAD and CGGP, click **DS Access**.
   - **6c** For each subcategory configure or verify the following selections:
     - Configure the following audit events
     - Success
     - Failure
   - **6d** (Conditional) For CGAD only, define the same configuration for all subcategories of **Account Management** and **Policy Change**.
7. (Conditional) For Windows Server 2008 and 2003, complete the following steps:
   - **7a** In **Security Settings**, expand **Local Policies** and click **Audit Policy**.
   - **7b** For CGAD and CGGP, click **Audit directory service access**.
   - **7c** Configure or verify the following selections:
     - Define these policy settings

- Success
- Failure

7d (Conditional) For CGAD only, configure or verify the same selections for **Audit account management** and **Audit policy change**.

8 Return to the command prompt, type `gpUpdate` and press **Enter**.

A.3 Configuring Active Directory Security Access Control Lists (SACLs)

The Security Access Control List (SACL) describes, in detail, the objects and operations to monitor. You must perform this configuration to generate events for operations that can result in, or are related to, changes in GPO data stored in Active Directory.

To monitor all changes of current and future objects inside Active Directory with Change Guardian for Active Directory, follow the steps in Section A.3.1, "Configuring SACLs for Change Guardian for Active Directory," on page 59. If you are running only Change Guardian for Group Policy in your environment, see Section A.3.2, "Configuring SACLs for Change Guardian for Group Policy Only," on page 60.

A.3.1 Configuring SACLs for Change Guardian for Active Directory

If you are running Change Guardian for Active Directory in your environment, complete the steps in this section. To monitor all changes of current and future objects inside Active Directory with Change Guardian, you must configure the domain node.

To verify or set this configuration:

NOTE: To use `adsiedit.msc` in Windows Server 2003, you must install the Windows Support Tools. For more information about installing Windows Support Tools, see http://technet.microsoft.com/en-us/library/cc755948%28WS.10%29.aspx.

---

1 Log on to a computer in the domain you want to configure using a user account with domain administrator privileges.

2 Open a command prompt, type `adsiedit.msc` and press **Enter** to start the ADSI Edit configuration tool.

3 Right-click **ADSI Edit**, and then select **Connect to**.

4 In the connection window, ensure **Name** is set to `Default naming context`, and **Path** points to the domain to configure.

NOTE: You must perform steps 5-15 three times, configuring the connection points for **Default naming context**, **Schema**, and **Configuration**.

---

5 In **Connection Point**, select **Select a well known Naming Context**, and then select one of the following:

- On the first time through this step, select **Default naming context** in the drop-down box.
- On the second time through this step, select **Schema**.
- On the third time through this step, select **Configuration**.

6 Click **OK**, and then expand **Default naming context** or **Schema** or **Configuration**.

7 Right-click the node under the connection point (begins with `DC=` or `CN=`), and select **Properties**.

8. On the Security tab, click **Advanced**.
9. On the Auditing tab, click **Add**.
10. Configure auditing to monitor every user.
    - ***If you are using Windows Server 2012,***
        1. Click **Select a principal**.
        2. Type `everyone` in the **Enter the object name to select** field.
        3. Click **OK**.
        4. In the **Type** field, select **All**.
        5. In the Permissions list, select the following:
            - Write All Properties
            - Delete
            - Modify Permissions
            - Modify Owner
            - Create All Child Objects

              The other nodes related to child objects are selected automatically.
            - Delete All Child Objects

              The other nodes related to child objects are selected automatically.
    - ***For all other versions of Windows,***
        1. Type `everyone` in the **Enter the object name to select** field.
        2. Click **OK**.
        3. In the Access list, select **Successful** and **Failed** for the following:
            - Write All Properties
            - Delete
            - Modify Permissions
            - Modify Owner
            - Create All Child Objects

              The other nodes related to child objects are selected automatically.
            - Delete All Child Objects

              The other nodes related to child objects are selected automatically.
11. In the **Applies to** or **Apply onto** field, select **This object and all descendant objects**.
12. Clear the setting to **Apply these auditing entries to objects and/or containers within this container only**.
13. Click **OK** until you close all open windows.
14. Repeat steps 5-13 two more times.

A.3.2 Configuring SACLs for Change Guardian for Group Policy Only

If you are running only the Change Guardian for Group Policy product in your environment, complete the steps in this section.

To verify or set this configuration:

NOTE: To use `adsiedit.msc` in Windows Server 2003, you must install the Windows Support Tools. For more information about installing Windows Support Tools, see http://technet.microsoft.com/en-us/library/cc755948%28WS.10%29.aspx.

---

1. Log on to a computer in the domain you want to configure using a user account with domain administrator privileges.
2. Open a command prompt, type `adsiedit.msc` and press **Enter** to start the ADSI Edit configuration tool.
3. Right-click **ADSI Edit**, and then select **Connect to**.
4. In the connection window, ensure **Name** is set to `Default naming context`, and **Path** points to the domain to configure.
5. In **Connection Point**, select **Select a well known Naming Context**, and then select **Default naming context** in the drop-down box.
6. Click **OK**, and then expand **Default naming context**.
7. Right-click the node under the connection point (begins with `DC=`), and select **Properties**.
8. Select the Security tab.
9. Click **Advanced**.
10. Click **Auditing**.
11. Click **Add**.
12. Configure auditing to monitor every user.
    - ***If you are using Windows Server 2012,***
        1. Click **Select a principal**.
        2. Type `everyone` in the **Enter the object name to select** field.
        3. Click **OK**.
        4. In the **Type** field, select **All**.
        5. In the Permissions list, select the following:
            - Delete
            - Create Organizational Unit objects
        6. In the Properties list, select the following:
            - Write gPLink
            - Write gPOptions
    - ***For all other versions of Windows,***
        1. Type `everyone` in the **Enter the object name to select** field.
        2. Click **OK**.
        3. In the Permissions list, select the following:
            - Delete
            - Create Organizational Unit objects
        4. In the Properties list, select the following:
            - Write gPLink
            - Write gPOptions
13. In the **Applies to** or **Apply onto** field, select **This object and all descendant objects**.

14. Clear the setting to **Apply these auditing entries to objects and/or containers within this container only**.
15. Click **OK** until you close all open windows.
16. In **Connection Point**, select **Select a well known Naming Context**, and then select **Configuration** in the drop-down box.
17. Click **OK**, and then expand **Configuration**.
18. Right-click the node under the connection point (begins with `CN=`), and select **Properties**.
19. Select the Security tab.
20. Click **Advanced**.
21. Click **Auditing**.
22. Click **Add**.
23. Configure auditing to monitor every user.
    - ***If you are using Windows Server 2012,***
        1. Click **Select a principal**.
        2. Type `everyone` in the **Enter the object name to select** field.
        3. Click **OK**.
        4. In the **Type** field, select **All**.
        5. In the Permissions list, select the following:
            - Delete
            - Create Sites Container objects
        6. In the Properties list, select the following:
            - Write gPLink
            - Write gPOptions
    - ***For all other versions of Windows,***
        1. Type `everyone` in the **Enter the object name to select** field.
        2. Click **OK**.
        3. In the Permissions list, select the following:
            - Delete
            - Create Sites Container objects
        4. In the Properties list, select the following:
            - Write gPLink
            - Write gPOptions
24. In the **Applies to** or **Apply onto** field, select **This object and all descendant objects**.
25. Clear the setting to **Apply these auditing entries to objects and/or containers within this container only**.
26. Click **OK** until you close all open windows.

B Configuring UNIX Operating System Auditing

Change Guardian requires you to enable the auditing system of your operating system. If you have already enabled auditing and Change Guardian is working as expected, then your operating system is properly configured. However, if you are not receiving events, use the information in this section to properly configure auditing for your operating system.

B.1 Configuring the AIX Audit Subsystem

The auditing subsystem on AIX computers stores files in the `/etc/security/audit` folder. You must have audit streaming enabled. However, streaming all events might consume too much space or processor time.

The following steps describe the minimum auditing activity Change Guardian requires.

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 the `/etc/security/audit/config` file includes the following stanzas:

   ```
   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/bincmds
   ```

3. Add the following events to all Change Guardian users:
   - 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

If you have unsuccessfully attempted to set up auditing on your AIX computer, ensure you remove all files in the `/etc/security/audit` folder except the `trail`, `stream.out` , and `bin` files.

B.2 Configuring the HP-UX Audit Subsystem

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

```
AUDITING=0

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 close -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 "

AUDEVENT_ARGS2=" "

AUDEVENT_ARGS3=" "

AUDEVENT_ARGS4=" "

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

B.3 Configuring the Solaris Auditing Subsystem

Versions 9 and 10 of the Solaris operating system have different auditing subsystems than Solaris version 11.

On computers running Solaris 9 or 10, perform the following steps:

1. Ensure the Basic Security Module will restart after reboot by running `./bsmconv` from the `/etc/security` folder.
2. Ensure 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 ps,as,cl,fd,fc,fm,fw

auditconfig -setnaflags ps,as,cl,fd,fc,fm,fw
```

B.4 Configuring a Linux Auditing Subsystem

Auditing subsystems on SUSE, Red Hat, and Red Hat variants are very similar. There are some differences in configuration based on operating system and on architecture. For Red Hat 4 and SUSE 10, configure the audit daemon in the `/etc/auditd.conf` and `/etc/auditd.rules` files. For Red Hat 5, Red Hat 6, and SUSE 11, configure the audit daemon in the `/etc/audit/auditd.conf` and `/etc/audit/auditd.rules` files.

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

1. (Conditional) For Red Hat and variants of Red Hat, ensure that the auditd service is enable by running the `chkconfig auditd on` command.
2. (Conditional) For SUSE, ensure that the auditd service is enable by running the `auditctl -e 1` command.
3. (Conditional) For computers that use a 32-bit architecture, add the following lines to the `audit.rules` file:

```
-a exit,always -F arch=b32 -S futimesat
-a exit,always -F arch=b32 -S unlinkat
-a exit,always -F arch=b32 -S fchownat
-a exit,always -F arch=b32 -S openat
-a exit,always -F arch=b32 -S exit
-a exit,always -F arch=b32 -S dup2
-a exit,always -F arch=b32 -S kill
-a exit,always -F arch=b32 -S rename
-a exit,always -F arch=b32 -S unlink
-a exit,always -F arch=b32 -S symlinkat
-a exit,always -F arch=b32 -S mount
-a exit,always -F arch=b32 -S fchmod
-a exit,always -F arch=b32 -S mknodat
-a exit,always -F arch=b32 -S execve
-a exit,always -F arch=b32 -S chown
-a exit,always -F arch=b32 -S open
-a exit,always -F arch=b32 -S exit_group
-a exit,always -F arch=b32 -S utime
-a exit,always -F arch=b32 -S adjtimex
-a exit,always -F arch=b32 -S chown32
-a exit,always -F arch=b32 -S renameat
-a exit,always -F arch=b32 -S close
-a exit,always -F arch=b32 -S creat
-a exit,always -F arch=b32 -S symlink
-a exit,always -F arch=b32 -S fchown
```

```
-a exit,always -F arch=b32 -S utimes
-a exit,always -F arch=b32 -S fchown32
-a exit,always -F arch=b32 -S link
-a exit,always -F arch=b32 -S settimeofday
-a exit,always -F arch=b32 -S fchmodat
-a exit,always -F arch=b32 -S lchown32
-a exit,always -F arch=b32 -S lchown
-a exit,always -F arch=b32 -S umount2
-a exit,always -F arch=b32 -S chmod
-a exit,always -F arch=b32 -S linkat
-a exit,always -F arch=b32 -S umount
-a exit,always -F arch=b32 -S fork
-a exit,always -F arch=b32 -S dup
-a exit,always -F arch=b32 -S mknod
-a exit,always -F arch=b32 -S vfork
```

4 (Conditional) For computers that use a 64-bit architecture, add the following lines to the `audit.rules` file:

```
-a exit,always -F arch=b64 -S futimesat
-a exit,always -F arch=b64 -S unlinkat
-a exit,always -F arch=b64 -S fchownat
-a exit,always -F arch=b64 -S openat
-a exit,always -F arch=b64 -S exit
-a exit,always -F arch=b64 -S dup2
-a exit,always -F arch=b64 -S kill
-a exit,always -F arch=b64 -S rename
-a exit,always -F arch=b64 -S unlink
-a exit,always -F arch=b64 -S symlinkat
-a exit,always -F arch=b64 -S mount
-a exit,always -F arch=b64 -S fchmod
-a exit,always -F arch=b64 -S mknodat
-a exit,always -F arch=b64 -S execve
-a exit,always -F arch=b64 -S chown
-a exit,always -F arch=b64 -S open
-a exit,always -F arch=b64 -S exit_group
-a exit,always -F arch=b64 -S utime
-a exit,always -F arch=b64 -S adjtimex
-a exit,always -F arch=b64 -S renameat
```

```
-a exit,always -F arch=b64 -S close
-a exit,always -F arch=b64 -S creat
-a exit,always -F arch=b64 -S symlink
-a exit,always -F arch=b64 -S fchown
-a exit,always -F arch=b64 -S utimes
-a exit,always -F arch=b64 -S link
-a exit,always -F arch=b64 -S settimeofday
-a exit,always -F arch=b64 -S fchmodat
-a exit,always -F arch=b64 -S lchown
-a exit,always -F arch=b64 -S umount2
-a exit,always -F arch=b64 -S chmod
-a exit,always -F arch=b64 -S linkat
-a exit,always -F arch=b64 -S fork
-a exit,always -F arch=b64 -S mknod
-a exit,always -F arch=b64 -S vfork
-a exit,always -F arch=b64 -S vfork
```