Contents

User Guide

NetIQ® Change Guardian™

October 2016

Legal Notice

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.

1 Introduction

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.

Change Guardian also helps you achieve compliance with regulatory and privacy standards, such as:

- Payment Card Industry Data Security Standards (PCI DSS)
- Health Insurance Portability and Accountability Act (HIPAA)
- International Organization for Standardization's latest standards (ISO/IEC 27001)

1.1 What is Change Guardian?

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 defend their critical systems and sensitive data.

Change Guardian provides the following 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.

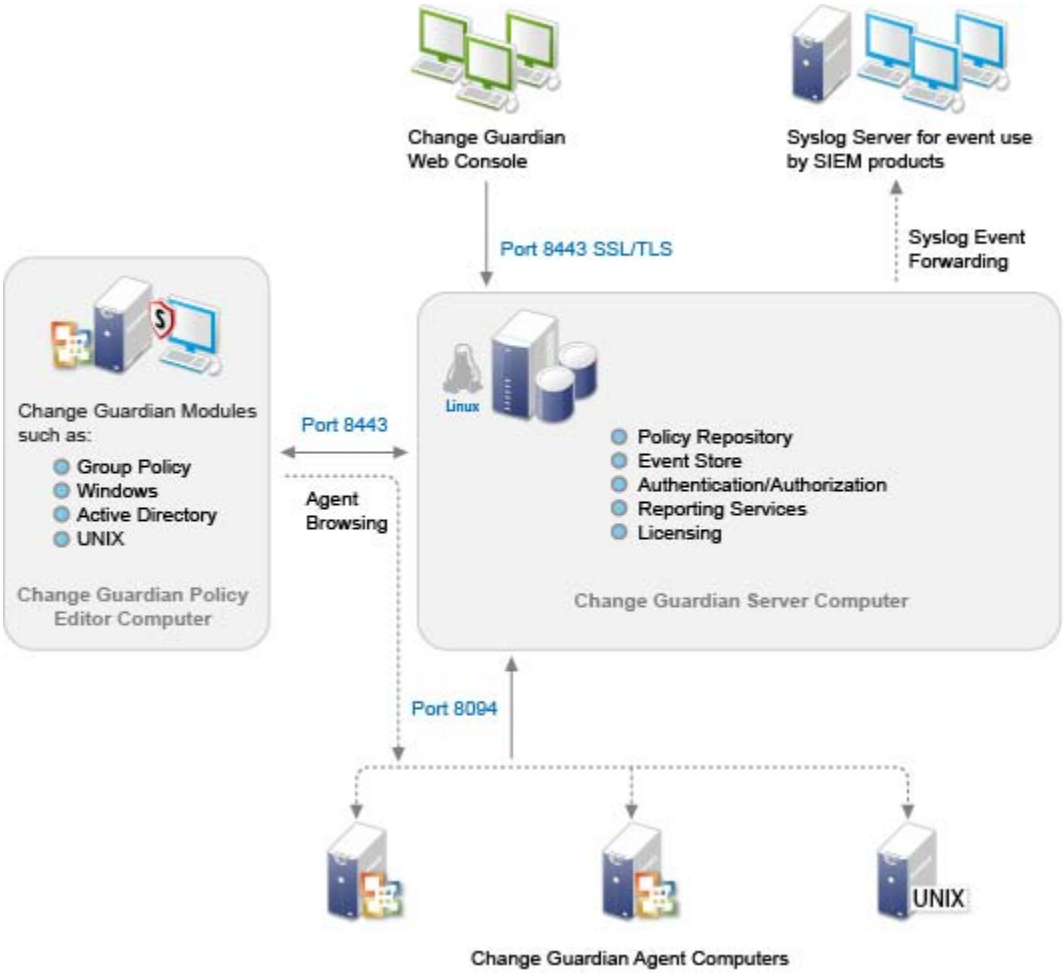
Change Guardian helps you reduce the time and complexity required to analyze disparate platform logs in the following ways:

- Centrally recording and auditing changes
- Creating intuitive monitoring policies through policy-based monitoring
- Automating daily change auditing and reporting

NetIQ Change Guardian also integrates with your existing security information and event management (SIEM) solution, such as NetIQ Sentinel. Change Guardian extends your SIEM solution's ability to detect and respond to threats by pinpointing the who, what, when, and where of an event while providing before and after values. 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 Understanding Change Guardian Components

Change Guardian includes a number of software components that you should plan to install strategically over a number of computers. The following diagram displays a traditional installation.



Change Guardian includes the following major 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 details that pinpoint 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 allows 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.

1.3 Default Ports

The Change Guardian server computer 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	Connects 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 retrieve their assigned monitoring policies.
	8443	Inbound	Required	Allows the Change Guardian server to receive events from monitored assets. **NOTE:** This port might 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.

Component	Ports	Direction	Required /Optional	Description
JAVOS	8094	inbound	Required	Allows the JAVOS service to accept connections from agents that are retrieving their assigned monitoring policies.
	9094	Inbound (loopback)	Required	Allows the Change Guardian server to call JAVOS on this port to signal/reset the event destination cache.
	9095	Inbound (loopback)	Optional	Allows users to see runtime metrics and active threads.
Active Directory Accounts/ LDAP Expander	8088	Inbound (loopback)	Required	Allows the Change Guardian server to retrieve information about Active Directory accounts.
	8089	Inbound (loopback)	Optional	Allows users to see runtime metrics and active threads.
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.
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.
Agent Manager	8082	Inbound	Required	Allows the agent to communicate with the Agent Manager.
	445	Outbound	Required	Allows the Agent Manager to deploy agents to Windows computers.

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 that 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 60-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 15. ◆ If you want to perform a traditional installation, see Section 2.2, “Traditional Change Guardian Server Installation,” on page 18. ◆ If you want to perform an appliance installation, see Section 2.3, “Appliance Change Guardian Server Installation,” on page 19.
❑	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 whether 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 *Security Agent for UNIX Configuration and Installation Guide*.
❑	(Conditional) If you want to monitor events on Windows computers, install the Windows agent. For more information, see Chapter 3, “Installing the Change Guardian Components,” on page 27.

2 Installing the Change Guardian Server

This chapter guides you through 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, “Understanding Change Guardian Components,” on page 10.

You can install the Change Guardian server on your own Linux-based server or deploy a ready-to-run appliance.

2.1 Planning for Change Guardian Server Installation

Before you install the Change Guardian server, verify hardware and software requirements and determine the resources you need for your Change Guardian implementation.

Change Guardian offers enhanced protection against security threats and compliance with United States federal government standards by supporting Federal Information Processing Standards (FIPS). For Change Guardian to run in FIPS mode, you must configure it after you install the Change Guardian server. For more information, see Section 2.4.7, “Configure Change Guardian to Run in FIPS Mode,” on page 23.

IMPORTANT: The installation process does not support installing the Change Guardian Server as a non-root user.

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 3 (64-bit)

  NOTE: The Change Guardian Server does not work on openSUSE.

- Red Hat Enterprise Linux for Servers (RHEL) 6.6 (64-bit)

  NOTE: Ensure the 64-bit `expect` RPM is installed before you start the installation process.

You can run the web console on the following supported browsers:

- Windows
  - Firefox version 5 and later

- Google Chrome
- Internet Explorer 10 and 11

- SLES

  Firefox version 5 and later

- RHEL

  Firefox version 5 and later

If the Internet Security Level in Internet Explorer is set to `High`, a blank page appears after logging in, 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 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 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 implementation:

Category	250 Monitored Assets	1000 Monitored Assets	2000 Monitored Assets
CPU	Two Intel Xeon 3-GHz (4 core) CPUs (8 cores total)	Two Intel Xeon 3-GHz (8 core) CPUs (16 cores total)	Two Intel Xeon 3-GHz (8 core) CPUs (16 cores total)
Memory	32 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 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 five days of local storage.
- In a primarily networked storage-only implementation, the amount of local storage can be minimized. However, due to decompression overhead, searching and reporting performance might 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 are 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.

2.1.4 RPM Requirements

The operating system for the Change Guardian server must include at least the Base Server components of the SLES server or the RHEL 6 server. Change Guardian requires the 64-bit versions of the following RPMs:

- bash
- bc
- expect
- coreutils

- gettext
- glibc
- grep
- libgcc
- libstdc
- lsof
- net-tools
- openssl
- python-libs
- samba-client
- sed
- zlib

2.2 Traditional Change Guardian Server Installation

You can install the 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 19.

To install the Change Guardian server interactively:

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

   ```
   tar zxvf cgserver-x.x.x-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 60-day evaluation license key included with the installer. This license key activates the full set of product features for a 60-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: Configuring FIPS using the custom configuration is not currently supported. For more information about configuring Change Guardian to run in FIPS mode, see Section 2.4.7, “Configure Change Guardian to Run in FIPS Mode,” on page 23.

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 that corresponds to the 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 you 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 `change_guardian_server_x.x.x.x.x86_64-0.xxxx.0.ovf.tar.gz`. The ISO file name is `change_guardian_server_x.x.x.x.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 change_guardian_server_x.x.x.x.x86_64-0.xxxx.0.ovf.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 the 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 that corresponds to the 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.

If you want Change Guardian to run in FIPS mode, you must complete additional steps. For more information, see Section 2.4.7, “Configure Change Guardian to Run in FIPS Mode,” on page 23.

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 that 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, “Understanding Change Guardian Components,” on page 10.

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.

2.4.7 Configure Change Guardian to Run in FIPS Mode

Change Guardian offers enhanced protection against security threats and compliance with United States federal government standards by supporting Federal Information Processing Standards (FIPS). Change Guardian leverages the FIPS 140-2 compliant features to meet the security requirements of United States federal agencies and customers with highly secure environments. Change Guardian is now re-certified by Common Criteria at EAL3+ and provides FIPS 140-2 Inside.

Complete the following procedure to configure Change Guardian to run in FIPS mode.

1 Ensure that Mozilla Network Security Services (NSS) and Mozilla NSS Tools are installed on the Change Guardian server.

2 From a command prompt on the Change Guardian server, change directory to `/opt/novell/sentinel/bin` and enter the following command:

```
./convert_to_fips.sh
```

3 Provide the requested input:

- **3a** When asked whether to backup the server, select **n**.
- **3b** Provide a password that meets the stated criteria. You will need this password later in this procedure.
- **3c** When asked whether to enter the external certificate in the keystore database, select **n**.
- **3d** When asked whether to restart the Sentinel server, select **y**.

4 Ensure that the `server0.0.log` file (located in `/var/opt/novell/sentinel/log`) contains the following entry:

```
Date_Timestamp|INFO|JAVOS listener|com.netiq.cg.capi.dao.UpgradeDao.upgrade
Upgrading EventDestination.Upgrade to fips compatible
Date_Timestamp|INFO|JAVOS listener|com.netiq.cg.capi.dao.UpgradeDao.upgrade
```

```
records updated=1 data={"service-
host":"Server_Name","password":"Encrypted_Password","protocol":"vosrestdispatc
her:rest
```

5 From a command prompt, change directory to `/opt/netiq/cg/javos/bin` and enter the following command:

```
./convert_to_fips.sh
```

6 Provide the password for the FIPS keystore database (the password you created in Step 3b on page 23).

7 When asked whether to restart the Java OS (javos) service, select **y**.

8 Ensure that the following entry is present in the `javos.log` file (located in `javos/log`):

```
Creating FIPS SSL listener on 8094
```

9 From a command prompt, change directory to `/opt/netiq/ams/ams/bin` and enter the following command:

```
./convert_to_fips.sh
```

10 Provide the requested input:

10a Provide the password for the FIPS keystore database (the password you created in Step 3b on page 23).

10b When asked whether to restart the Agent Manager service, select **y**.

11 Ensure that the `ams.log` file (located in `ams/log`) contains the following entry:

```
INFO [Date_Timestamp,446] com.netiq.commons.security.FIPSProvider: Running in
FIPS mode. Changing the SSL security provider from JSSE to FIPS. /opt/netiq/
ams/ams/security/nss
```

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 Customer Center, which hosts appliance updates, and provides key 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 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 Configuring the Appliance with SMT in the *NetIQ Sentinel Installation and Configuration Guide*.

3 Installing the Change Guardian Components

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

3.1 Policy Editor Computer Requirements

The following table lists the requirements and recommendations for computers running the Policy Editor:

Category	Requirement
Operating System	One of the following: ◆ Windows 10 (32- and 64-bit) ◆ Windows 8 (32- and 64-bit) ◆ Windows 7 (32- and 64-bit) ◆ Windows Server 2012 R2 ◆ Windows Server 2012 ◆ Windows Server 2008 R2
Additional Software	◆ Microsoft .NET Framework 4.0 Extended or later ◆ Microsoft .NET Framework 3.5 Service Pack 1 ◆ (Optional) Change Guardian Windows agent * * To enable browsing for Windows data sources while creating a policy, the computer where you install the Policy Editor must have an agent. If you do not install an agent on the Policy Editor computer, you must manually enter the data source paths while creating a policy.

3.2 Installing the Policy Editor

The Policy Editor interface lets you configure monitoring policies and assign monitoring policies to monitored computers.

To install the Policy Editor:

1. In a web browser, access the Change Guardian web console at `https://server:8443`, where *server* is the IP address of the Change Guardian server.
2. When prompted, provide your Change Guardian user name and password.
3. Click **Integration**, and then click **Agent Manager**.
4. Click **All Assets**, and then click **Manage Installation** and select **Download**.
5. Select **Change Guardian Policy Editor**, and then click **Start Download**.

   Agent Manager downloads `ChangeGuardianPolicyEditor.zip` to your computer.
6. Copy `ChangeGuardianPolicyEditor.zip` to the computer where you want to install the Policy Editor and extract the files.

   The package includes `NetIQCGPolicyEditorInstaller.exe` and `NetIQCGPolicyEditorInstaller.config`. Both files must be in the same directory.
7. Log in to the computer where you want to install the Policy Editor with an administrator account.
8. Run the installation program, `NetIQCGPolicyEditorInstaller.exe`, and follow the instructions.
9. When the installation completes, click **Finish**.

3.3 Installing the Windows Agent

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

- Remotely install agents using the NetIQ Agent Manager. For more information, see Section 3.3.1, “Remotely Install the Windows Agent,” on page 29.
- Silently install the agent. For more information, see Section 3.3.2, “Performing a Silent Agent Installation,” on page 30.

The following table lists the requirements and recommendations for computers where you plan to install the agent:

Category	Requirement
Operating System	One of the following: ◆ Windows 10 (32- and 64-bit) ◆ Windows 8 (32- and 64-bit) ◆ Windows 7 (32- and 64-bit) ◆ Windows Vista (32- and 64-bit) ◆ Windows Server 2012 R2 ◆ Windows Server 2012 ◆ Windows Server 2008 R2 ◆ Windows Server 2008 (32- and 64-bit) ◆ Windows Server 2003 R2 (32- and 64-bit)
Additional Software	◆ Microsoft .NET Framework 4.0 Extended or later ◆ Microsoft .NET Framework 3.5 Service Pack 1

3.3.1 Remotely Install the Windows Agent

Remote installation using the NetIQ Agent Manager provides a convenient and uniform method for installing one or more Windows agents.

To remotely install agents, you must first add the assets (computers) where you want to install agents. You can import assets from Active Directory or a text file, or manually add assets. After you add assets, select the assets to which you want to deploy agents and then install the agents.

To add assets to Agent Manager:

1. In a web browser, access the Change Guardian web console at `https://server:8443`, where *server* is the IP address of the Change Guardian server.
2. When prompted, provide your Change Guardian user name and password.
3. Click **Integration**, and then click **Agent Manager**.
4. Do one of the following:
   - (Conditional) If you have not previously added assets, in Agent Manager, under **Asset Groups**, click **All Assets** and then click **Add Assets**.
   - (Conditional) If you previously added assets, in Agent Manager, click **All Assets**, then **Manage Assets**, and then **Add**.
5. (Conditional) If you want to import assets from Active Directory, complete the following:
   - **5a** Click **Active Directory**.
   - **5b** Provide the domain name or IP address of the Active Directory server and credentials for connecting to the server, and then click **Authenticate**.
   - **5c** Navigate the Active Directory tree to locate the assets you want to add, select the assets, and then click **Add Assets**.
6. (Conditional) If you want to import assets from a text file, complete the following:
   - **6a** Create a text file with a header line containing the columns `Hostname`, `MajorType`, and `Addresses`. Use a tab to separate the columns. In the `Hostname` column, type the fully-qualified domain names of the computers where you want to deploy agents. Optionally, you can specify the IP addresses in the `Addresses` column. In the `Major Type` column, specify whether the operating system is UNIX or Windows. For example:

Hostname	MajorType	Addresses
houidam101.us.netiq.corp	Windows	
houidam102.us.netiq.corp	Windows	10.204.102.5

   - **6b** In the Agent Manager, click **Hosts List**.
   - **6c** Click **Browse**, navigate to the location where you saved the text file, and then click **Open**.
7. (Conditional) If you want to manually add an asset, do the following:
   - **7a** Click **Host**.
   - **7b** Specify the host name or IP address of the computer. To specify multiple IP addresses, use a comma to separate the addresses.
   - **7c** Select the appropriate operating system type.
   - **7d** Click **Add Assets**.

You can now select the assets where you want to deploy agents and install the agents.

To deploy Windows agents to assets:

1. From the assets list, select the computer where you want to deploy an agent. You can select multiple computers if Agent Manager can use the same credentials to connect to the computers.
2. Click **Manage Installation**, and then click **Install or Upgrade Agents**.
3. Provide credentials for an account that can connect to the computer and then click **Next**.

   The account must be the local administrator account or a domain account in the Local Administrators group.
4. For the agent revision, select **NetIQ Change Guardian Agent for Windows *Agent Version***, where *Agent Version* is the version of the agent you want to deploy.
5. Select the configuration to use for the deployment, or click **Add** to specify a new configuration.
6. Click **Start Installation**.

Agent Manager initiates the installation. Use the **In progress Tasks**, **Completed Tasks**, and **Failed Tasks** tabs to monitor the progress.

NOTE: When you use Agent Manager to install Windows agents, Agent Manager also installs the NetIQ Client Agent Manager component on the selected assets.

3.3.2 Performing a Silent Agent Installation

You can use the Agent Manager to download a silent installation package that contains the files necessary to install the Windows agent without having to interact with the setup program.

To silently install the Windows agent:

1. In a web browser, access the Change Guardian web console at `https://server:8443`, where *server* is the IP address of the Change Guardian server.
2. When prompted, provide your Change Guardian user name and password.
3. Click **Integration**, and then click **Agent Manager**.
4. Click **All Assets**, and then click **Manage Installation** and select **Download**.
5. Select the package you want to download and the configuration you want to use, and then click **Start Download**.

   Agent Manager downloads `ChangeGuardianAgentforWindows.zip` to your computer.
6. Copy `ChangeGuardianAgentforWindows.zip` to the computer where you want to install the Windows agent and extract the files.

   The silent installation package includes `NetIQCGAgentSilentInstaller.exe` and `NetIQCGAgentSilentInstaller.config`. Both files must be in the same directory. The configuration file contains the configuration you chose when you downloaded the silent installation package.
7. From a command prompt with the **Run as administrator** option, change directory to the location where you extracted the files and run `NetIQCGAgentSilentInstaller.exe`.

3.4 Accessing the Policy Editor

When you start the Policy Editor you must connect to the Policy Repository, which runs on the Change Guardian server, with an account that is a member of the Administrator or Change Guardian Administrator role.

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, all available modules are installed automatically. Then 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.

3.6 Using the Security Agent for UNIX

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

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

The Security Agent for UNIX helps you effectively address these challenges by enabling NetIQ Change Guardian to monitor the configuration and risk compliance of your UNIX and Linux environments.

For more information about Security Agent for UNIX, see Security Agent for UNIX documentation.

4 Setting Up Your Environment for Monitoring

This chapter guides you through using the Change Guardian Policy Editor to perform the following tasks:

- Create policies and policy sets
- Assign policies and policy sets to the computers and asset groups in your enterprise
- Set group membership
- Create reports

4.1 Understanding Policies

Policies allow you to define how Change Guardian monitors assets in your environment. 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

Each Change Guardian module includes several policy types for the respective platforms they support.

After you create a policy, Change Guardian saves the policy in the Policy Repository on the Change Guardian sever computer. If you make changes to the policy later, Change Guardian creates a new **revision** of that policy. Policy revisions allow you to keep and share works in progress. Use the Policy Repository to view all policy revisions as well as the version number of the currently loaded policy. You can also load a previous revision of a policy to edit or enable.

4.1.1 Creating Policies

You can create a policy in the following ways:

- Create a brand new policy with no pre-configured settings
- Clone and customize an out-of-the-box template
- Clone and customize an existing policy

Creating a Policy

To create a policy:

1. In the left pane of Policy Editor, select one of the following:
   - Active Directory
   - Group Policy
   - UNIX
   - Windows
2. Expand the list of policies and select the policy type you want to create, such as **Activity Directory Policies > AD Object**.
3. Click **Create Policy**.
4. On the policy details window, make the appropriate changes.
5. (Conditional) If you are creating a Windows policy to monitor Local Users and Groups, complete the following:
   1. To ensure the policy generates events, you must add at least one of the following:
      - Event List
      - LGU Privileges
   2. Select the events and/or privileges you want to monitor.
6. Click **Submit**.
7. (Conditional) If you want to enable the policy now, select the **Enable this policy revision now** checkbox.

NOTE: For more information about enabling a policy, see Section 4.1.5, “Enabling a Policy Revision,” on page 36.

Cloning a Template

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.

To clone an out-of-the-box template:

1. In the left pane of Policy Editor, select one of the following:
   - Active Directory
   - Group Policy

- UNIX
- Windows

2 Expand the list of templates and select the template you want to clone. For example, **Active Directory Templates > AD Object > Site Link Cost Modified**.

3 Click **Apply**.

4 On the policy details window, make the appropriate changes, and then click **Submit**.

5 (Conditional) If you want to enable the policy now, select the **Enable this policy revision now** checkbox.

NOTE: For more information about enabling a policy, see Section 4.1.5, “Enabling a Policy Revision,” on page 36

Cloning a Policy

Cloning an existing 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 revision of the selected policy when creating a clone, but you can select a specific policy revision.

4.1.2 Understanding Event Severity

When you create or edit a policy, you can specify a constant severity level or allow Change Guardian to calculate the severity automatically. If you set **Severity** to `Automatic`, Change Guardian calculates the severity based on whether the user is authorized and if the action was successful. For example:

- **Sev 5.** Unauthorized user, successful action
- **Sev 4.** Unauthorized user, failed action
- **Sev 3.** Authorized user, failed action
- **Sev 2.** Authorized user, successful action
- **Sev 0 or 1.** System events

4.1.3 Understanding Managed Users

When you create or edit a policy, the **Managed Events** section allows you to specify the managed users for that policy. Managed users are allowed to make specific changes to the asset the policy monitors. When managed users make changes, the generated events appear as managed change events.

If you specify a user group as a managed user, as group membership changes, Change Guardian synchronizes policies with the new group members. For more information, see Section 4.4, “Understanding LDAP Settings,” on page 38.

4.1.4 Understanding Event Context

When you create or edit a policy, use the **Event Context** section to categorize the policy and specify its purpose. Generated events include the event contexts you specify. You can select one or more of the following default event contexts:

- **Risk Domain.** Select a specific value, or create your own.
- **Risk.** Select a specific value, or create your own.

- **Sensitivity.** Select a specific value, or create your own.
- **Regulation/Policy.** Select a specific value, or create your own.
- **Control/Classification.** Create your own user-defined value.
- **Response Window.** Create your own user-defined value.

You can also create new event contexts with user-defined values.

4.1.5 Enabling a Policy Revision

Before you can assign a policy revision to monitor computers or asset groups, you must enable it. You can enable a policy revision in the following ways:

- You can enable a policy when you submit it to the Policy Repository, after creating or editing it.
- You can enable a submitted policy revision from the selected module window.

After you enable the policy revision, Change Guardian sends the policy to assigned assets.

If you modify and enable a policy revision already assigned to computers, Change Guardian updates that policy to all computers with the policy assigned. When you update the enabled revision of a policy, Change Guardian automatically updates any monitored assets that have that policy assigned with the new revision.

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

To enable a policy revision from a module window:

1. In the left pane, select the policy.
2. On the **History** tab, select the policy revision you want to enable.
3. Click **Enable**.

4.1.6 Exporting and Importing Policies

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.

4.2 Understanding Policy Sets

Policy sets combine multiple policies from one or more Change Guardian modules, allowing you to organize and manage monitoring needs for a specific use case. You can include a policy in multiple policy sets, which reduces the total number of policies in the system.

If you add a policy to a policy set that contains multiple asset types, the policy applies only to the applicable assets. For example, if you apply a UNIX policy to a policy set that contains Windows and UNIX assets, the policy applies to the UNIX assets only.

Use the Policy Set Manager to add, edit, or clone policy sets.

To access the Policy Set Manager:

1. In the left pane, select **NetIQ Change Guardian**.
2. Select **Policy Set Manager**.

After you create a policy set, you can assign the set as you would assign a policy. For more information, see Section 4.6, “Assigning Policies and Policy Sets,” on page 39.

4.3 Understanding Event Destinations

An **event destination** is where Change Guardian sends incoming events for a particular policy. You can view information about access and changes to critical files, systems, and applications. It is also where you deploy alert rules to notify you of those changes. For more information about alerts, see Chapter 6, “Understanding Alerts,” on page 47.

A policy must have at least one event destination. When you create a policy, it automatically uses the default event destination. When you install Change Guardian, the default event destination is the Change Guardian server. You can create and assign additional event destinations to meet your environment and regulatory needs. You can also change the default event destination setting.

If you set another event destination as the default, all new policies automatically use the new default location. Existing policies will continue to use their previously assigned event destinations. To change the event destinations for existing policies, see “Assigning Event Destinations to Policies” on page 38.

If your environment has multiple event destinations, and the default event destination is FIPS-enabled, some additional configuration steps are required. For more information, see Section 6.2.3, “Ensuring Alternate Event Destinations Receive Alerts,” on page 49.

4.3.1 Creating an Event Destination

You can create event destinations using one of the following models:

- **REST Dispatcher.** Sends events to Change Guardian server or NetIQ Sentinel.
- **Syslog Dispatcher.** Sends events to third-party SIEM or syslog server.

To create an event destination:

1. Log in to the Policy Editor.
2. Select **Settings > Event Destinations**.
3. Click **Add**.
4. Specify a unique name for the event destination.
5. Specify one of the event destination models.
6. Provide system information for the server where you want to send events.
7. (Optional) If you want to send Change Guardian system events that only match specific criteria, select the checkbox above the filter drop-down list, and provide filter criteria.

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

4.3.2 Assigning Event Destinations to Policies

When you create a policy, it automatically uses the default event destination. If you want to send event data to another destination, add an event destination to the policy (or policy set). The new event destination can be either in addition to or instead of the default event destination. The updated event destination setting will take effect at the next heartbeat interval, when the asset computer reads the updated policy information.

To assign event destinations to a policy:

1. Log in to the 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 one or more event destinations to assign to the specified policy or policy set.
6. Click **OK**.

4.4 Understanding LDAP Settings

Change Guardian uses LDAP to process each user group in a policy as a list of the group members. For example, if a policy monitors Group A, LDAP allows Change Guardian to monitor the activity performed by the individual users in Group A. If the policy returns an event, the name of the user performing the change is included in the event report.

You must configure LDAP settings for every grouped resource you intend to monitor. If you do not configure LDAP settings for a grouped resource, and you specify that grouped resource in a policy, the Policy Editor submits the policy to the Change Guardian server, but the policy cannot monitor the group members correctly.

To access LDAP settings, click **Settings > LDAP Settings**.

The LDAP Settings window displays the domain name for each resource. From this window, you can create, edit, and delete settings.

NOTE: You cannot delete a setting that an active policy is using.

When you create or edit a setting, you define the domain, the credentials to allow access to group information, and the polling interval.

4.5 Understanding and Managing Asset Groups

Asset groups allow you to perform the following tasks:

- Categorize computers
- Assign policies to the group instead of to each individual computer. When you add a new computer to the group, Change Guardian automatically deploys the policies assigned to the group to the new computer.

To work with asset groups, in the left pane, select **NetIQ Change Guardian**, and then select **Asset Groups**. You can choose one of the following views:

- **Asset Groups** (default view) displays all asset groups and the computers they contain. To view the members of the group, click the **Membership** tab.

  Change Guardian supports the following types of asset groups:

  - **Default groups** match specific platforms. You can view the members of default groups, but you cannot modify or delete the groups.
  - **Static groups** contain only the assets you manually add to them. To add or remove members, you must manually update the group.
  - **Dynamic groups** contain all assets that match the filter criteria you specify for the group. You can modify the filter criteria, but you cannot add or remove specific assets manually. Every 30 minutes, Change Guardian refreshes the group membership according to the specified criteria.
- **Assets** displays a list of all computers with Change Guardian agents installed. On the **Attributes** tab, you can view the computer attributes, such as computer name and operating system, and the groups to which the computer belongs. If you have the appropriate permissions, you can use the **Membership** tab to modify the computer's membership in static asset groups.

You can filter the assets or asset groups to see only the items that meet certain criteria. Expand **Filter Values**, and then use any combination of the available conditions. Specify values for the conditions you select, and then click **Apply**.

4.6 Assigning Policies and Policy Sets

Policies are stored in the Change Guardian Policy Repository and are available to the Change Guardian users in your enterprise to assign to computers and asset groups.

Use the Policy Assignment screen to assign policies and policy sets to the assets or asset groups in your enterprise. 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.

4.7 Understanding Monitoring Schedules

By default, Change Guardian policies monitor computers and asset groups continuously. A **monitoring schedule** allows you to define specific times when a policy or policy set monitors computers and asset groups. For example, you can suspend monitoring during scheduled maintenance times, which eliminates events generated as a result of the maintenance. When you assign a policy or policy set to an asset or asset group, you can attach a monitoring schedule.

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

Examples of valid time restrictions include:

- Mondays, Tuesdays, and Wednesdays from 3-5 p.m.
- Mondays from 3-5 p.m. and Tuesdays from 4-6 p.m.
- Mondays from Midnight-7 a.m., 9 AM-2 p.m., and 6 p.m.-Midnight

To create a monitoring schedule:

1. Log in to the Policy Editor.
2. Click **Settings > Schedule Monitoring Time**.

3. Click **Add**.
4. In the **Schedule Time** window, select the time(s) and day(s) 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.

5. Click **OK**.

4.8 Understanding Change Guardian Email Alerts

Change Guardian can send email notifications for events to specified administrators and operators. To enable email alerts:

- Install an email server on each event destination computer in your Change Guardian environment.
- Use the Policy Editor to:
  - Add each email server to Change Guardian.
  - Create one or more notification groups for each email server.
- Use the Change Guardian web console to assign email alerts to specified events. For more information, see Section 5.8, "Assigning Email Alerts to Events," on page 45.

4.8.1 Adding Email Servers to Change Guardian

After you ensure each event destination computer in your Change Guardian environment hosts an email server, you can add each email server to Change Guardian.

To add an email server to Change Guardian:

1. In the Policy Editor, select **Settings > Email Configuration**.
2. Under **Email Servers**, click **Add**.
3. Specify the name and description of the email server you want to add.
4. Specify values for the following fields:
   - **SMTP Host.** The fully qualified domain name of the email server computer.
   - **SMTP Port.** The remote SMTP port to use when communicating with the email server computer.
   - **Secure.** Specifies whether the connection to the SMTP computer must be a secure connection. If **Yes**, specify the protocol type.

     If you select **No**, the **SMTP Port** will be set to **25** by default.

     If you select **Yes**, the **Protocol** attribute is displayed.
   - **From.** The return email address appearing on each email alert for this email server.
   - **Authentication Required.** Specifies whether the email server requires SMTP authentication to send email. If **Yes**, specify the following:
     - **User Name.** The user name to use when connecting to the SMTP server.
     - **Password.** The password corresponding to the specified SMTP user name.
   - **Protocol.** Specifies which protocol can be used for the email communication. You can select **SSL** or **STARTTLS**.

NOTE: If you select **SSL**, the **SMTP Port** value must be set to **465**.

If you select **STARTTLS**, the **SMTP Port** value must be set to **587**.

4.8.2 Creating and Configuring Notification Groups

For each email server you add to Change Guardian, you must create one or more notification groups specific to that email server. A notification group specifies one or more 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 the notification groups available for that email server. For more information, see Section 5.8, “Assigning Email Alerts to Events,” on page 45.

To create and configure a notification group:

1. In the Policy Editor, select **Settings > Email Configuration**.
2. Select the email server for which you want to create a notification group.
3. Under **Notification Groups**, click **Add**.
4. Specify the name and description of the notification group you want to create.
5. Specify values for the following fields:
   - **From.** The return email address appearing on each email alert for this email server.
   - **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 for the alert email.
   - **Maximum Events per Email.** Specifies the maximum number of events in the email alert.
   - **Include Change Details.** Specifies whether the body of the email contains the details of the change detected by Change Guardian.
   - **Email Format.** Specifies either text or HTML.

4.9 Using Change Guardian Administrative Reports

Change Guardian allows you to create custom reports with details about the configuration for your environment. 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.

5 Viewing Change Guardian Events

This chapter describes using the Change Guardian web console to view **events**, which are the results from assigned policies and policy sets, in event reports. 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, specify your Change Guardian user name and password.

5.1 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 11 or later
- Mozilla Firefox 47 or later
- Google Chrome 51

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

- Security level is Medium-high. If the security level is High, the web console displays a blank page.
- Compatibility View is disabled.
- Automatic prompting for file downloads is enabled. Enabling this option ensures a pop-up blocker does not prevent the file download.

5.2 Understanding Event Information

By default, the Change Guardian web console displays events with all severity levels, allowing you to view the following information for each event:

- The specific alert severity

- Either of the following:
  - The name of the file changed or accessed
  - The name of the Active Directory object changed
- Either of the following:
  - The computer on which that file resides
  - 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 related to binary files include only delta information.

5.3 Viewing Detailed Event Information

The Change Guardian web console allows you to schedule reports and see additional detail for each event.

To see detailed event information, click the shield icon.

5.4 Reporting

The Change Guardian web console includes a report for policy events. When you run the report, you can accept or customize the default options, including:

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

5.5 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" in the *NetIQ Sentinel Administration Guide*.

5.6 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.

5.7 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 at any time to quickly perform a search instead of manually building the query again.

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

5.8 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 server configured for the web console computer. If you do not have an email server configured, no notification groups appear as available actions for the event routing rule. For more information about configuring email servers, see Section 4.8, "Understanding Change Guardian Email Alerts," on page 40.

To assign email alerts to an event:

1. Log in to the Change Guardian web console.
2. Click **Routing**, and then click **Create**.
3. Specify 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.
4. 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.

5.9 Forwarding Events for Long-Term Retention

Change Guardian stores raw data and compressed event data on the local file system. You can configure Change Guardian 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, which the Change Guardian administrator configures. 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*.

6 Understanding Alerts

Everything that happens in your environment creates an event. Most events are everyday occurrences and do not require any action on your part. A set of similar or comparable events in a given period, however, might indicate a potential threat. For example, a change to the Windows file system or multiple failed logins within a specified time frame. Change Guardian uses alert rules to help you take appropriate actions to mitigate any problems. To receive instant notification about such potential threats, you can configure alert rules to create alerts.

6.1 Overview

The following provides an overview of creating and monitoring alerts:

1. Configure alert rules to create alerts when a matching event occurs.

   An alert contains almost the same information as the related event and also includes additional information specific to the alert, such as owner, state, and priority.

   As Change Guardian detects subsequent instances of the same alert, the product associates the trigger events to the existing alert to avoid duplication of alerts.
2. View and monitor alerts in the Change Guardian web console. As you monitor alerts, you can assign alerts to different users and roles, track the alert from origination to resolution, and annotate the alert rule by adding information to the knowledge base.
3. Configure alert retention policies to specify when to automatically close and delete the alerts from Change Guardian.

6.2 Managing Alert Rules

The Alert Rules window in the Policy Editor allows you to:

- Create alert rules
- Edit alert rules
- Delete alert rules
- Redeploy alert rules
- View the status of alerts

On the Alert Rules window, you can choose one of the following views:

- All alert rules
- Alert rules grouped according to the associated event destination

To access the Alert Rules window, on the Settings menu, click Alert Rules.

Change Guardian automatically associates the relevant events and identities with the alert to help you determine the root cause of potential threat. For example, you can create an alert rule to alert you when the same user violates the same policy a specified number of times on the same asset within a specified time frame.

NOTE: If you are using Change Guardian in a mixed environment with NetIQ Sentinel, the alert rules you create in Change Guardian are available as correlation rules in the Sentinel web console. For best results in a mixed environment, use Sentinel to manage these rules.

6.2.1 Creating an Alert Rule

When you create an alert rule, specify the following:

- The policy or policies you want to monitor for events. If you do not specify one or more policies, the alert rule creates an alert for all events for all policies.
- An optional pattern the events must match before the alert rule creates an alert. For example, if you monitor the policy name for `DNS`, the alert rule creates alerts for all policies that contain `DNS` in the policy name, such as `DNS Configuration` and `Process and DNS`.
- Whether you want to monitor managed or unmanaged users.
- Alert criteria that further define the specific circumstances under which the alert rule creates an alert for the specified policies:
  - Generate an alert when an event occurs a specified number of times in a specified time frame.
  - Group alerts according to the specified event attribute.
- The event destinations to which you want to deploy the alert rule. By default, all available event destinations are selected.

By default, when you create an alert rule, Change Guardian uses the user account associated with the event destination, which is typically the `eventdispatcher` user. This user account has the `Manage correlation rule` permission. If a user creates an event destination and associates a different user account, that account must have the `Manage correlation rule` permission.

NOTE: The alert rule name supports only alphanumeric characters and underscores. Special characters, such as `-!`~#$%^&()+=[],;.` and space, are not supported.

For more information about event destinations, see Section 4.3, “Understanding Event Destinations,” on page 37.

6.2.2 Redeploying Alert Rules

When you create an alert rule, Change Guardian automatically deploys the alert rule to the event destination you specify.

If you make changes to the alert rule, such as modifying its alert criteria or adding information to the knowledge base, you can redeploy it to the event destination. Redeploying an alert rule ensures the event destination has the most recent version of the alert rule. For more information about the alert knowledge base, see “Viewing Alerts” on page 50.

6.2.3 Ensuring Alternate Event Destinations Receive Alerts

To ensure alert rules on the alternate event destinations generate alerts when the default event destination is FIPS-enabled, you must replicate the certificates from the alternate event destination to the default event destination.

1. Download the certificates from the alternate event destination to the default event destination server, and place them in a temporary location, such as `/tmp`.
2. Change the credentials as follows:
   - `# chown novell:novell /path to certificate`
   - `# chmod 644 /path to certificate`
3. Open a command prompt and go to `/opt/novell/sentinel/bin`.
4. Run the following command for all alternate event destinations:

   `./convert_to_fips.sh -i /path to certificate`
5. Restart the default event destination server.

6.3 Managing Alerts

Alerts notify you of what is most important. Using the Change Guardian web console, users can quickly triage alerts and determine which ones need a response.

For example, during the typical life cycle of an alert, a user will:

- Open an alert view and either pick an alert already assigned to them or claim an unassigned alert.
- View the alert details, such as the metadata, information about the alert rule that generated the alert, the triggering event and its identity information, and any knowledge base information associated with the alert.
- Determine the next step and add comments about the decision:
  - Close as harmless
  - Respond appropriately, and then close
  - Investigate further

You can also define rules to store only specific alerts in the database so that the database does not get overloaded. You can also define retention policies to automatically close and delete alerts after a specific duration.

6.3.1 Viewing and Triaging Alerts in Alert Views

Real-time alert views in the Change Guardian web console show you the alerts that are most important to look at and enable you to view and manage alert details. Charts provide a summary of alerts and the table provides a prioritized list of all the alerts. Alert views also allow you to perform alert triage operations such as changing states of an alert, assigning alerts to users or roles, adding information to the knowledge base, and so on. You can further drill down into each alert to view the alert details such as trigger events, user identities involved, and alert history.

To view and analyze alerts, you must first create an alert view.

Creating an Alert View

To create an alert view, you must either be an administrator or have the Manage Alerts permission.

To create an alert view:

1. Log in to the Change Guardian web console.
2. Click **Real-time Views > Alert Views >** the **Create** icon.
3. Specify the following:
   - Name
   - Sharing (public or private)
   - Data sources from which to view alerts
   - Filter criteria
   - Time range for which to view alerts
   - Alert period (created or modified)
4. Save the alert view.

Viewing Alerts

Change Guardian provides a tabular representation of alerts that matches the specified alert criteria. The charts represent the alerts overview information classified by Priority, State, and Severity. The alert view table displays only distinct alerts. Duplicate alerts are rolled up to a single distinct alert. The alert view table provides information about an alert such as severity, priority, owner, state, occurrences, and so on.

IMPORTANT: The alerts are stacked based on the event fields and their values. The alerts are not stacked by time.

The **Last Modified** field will display the alert management activity. If you modify the owner, priority, or state of the alert, **Last Modified** field will be updated with the new timestamp.

To view alert views:

1. In the Change Guardian web console, click **Real-time Views > Alert Views**.
2. Select the desired alert view and click the **Open the alert view** icon.

As you monitor alerts, you can perform the following activities in the alert view:

- Mouse over the charts to determine the number of alerts based on alert states, priority, and severity.
- Sort alerts based on one or more columns in the table. Press Shift+click to select multiple columns to sort. By default, the alert view table displays alerts based on the time when the alerts were triggered. Therefore, the latest alerts are listed on the top in the table.
- Assign alerts to a user or a role, including yourself or your role.
- Modify the alert state to indicate the progress on the alert investigation.
- Add comments to the alert to indicate the changes you made to the alert, which helps you to keep an up-to-date record of the alert investigation. For example, you can add comments when you change the state of a specific alert or when you have gathered more information about the alert. Providing specific comments allows you to accumulate knowledge about a particular

instance of the alert and track how a particular condition was addressed. Comments are important in tracking the alert, particularly if the process of resolving the alert spans several users or roles.

- View events that triggered the alert and drill down further to the extent of viewing the user identities that triggered the event by clicking the **View details** icon in the alert view table.

  The Alert Details page displays a detailed information about an alert including the following:

  - **Source:** Displays the alert rule that generated the alert. You can also annotate the alert rule by adding information to the knowledge base so that future alerts generated by this alert rule include the associated historical information.
  - **Knowledge Base:** The knowledge base is a repository that contains information about the conditions that resulted in the alert. It can also include information about resolution of a particular alert, which can help others resolve similar alerts in the future. Over time, you can collect a valuable knowledge base about the alert specific to a tenant or an enterprise.

    For example, an employee has recently joined the organization and is supposed to have the access permissions to a secured server. But this employee might not have been added yet to the authorized users list. Therefore, an alert is generated every time the employee tries to access the server. In such a case, you can add a note in the alert knowledge base to indicate that the “employee is approved to access the server, but is not yet listed in the authorized users list. This alert can be ignored and set to low priority.”

    NOTE: To view or edit the knowledge base, you must be an administrator or have the **View Knowledge Base** or **Edit Knowledge Base** permissions.

  - **Alert Fields:** Displays the alert fields that provide the following information:
    - who and what caused the alert.
    - the assets affected.
    - the taxonomic categories of the action that caused the alert, the outcome, and so on. For more information on taxonomy, see Sentinel Taxonomy.
  - **Trigger Events:** Displays the events that triggered the correlated event associated with the alert. You can determine the conditions that triggered the alert by examining the trigger events.
  - **Show history:** Displays the changes made to the alert, which helps you track any actions taken on the alert.
  - **Identities:** Displays the list of users involved in the alert. This information helps you to investigate the users involved in the alert and monitor their activities.

6.3.2 Analyzing Alert Dashboards

If you are using a mixed environment with Change Guardian and Sentinel, you can use the alert dashboard in Sentinel to see a high-level overview of the alerts in your organization. The alert dashboard enables you to analyze and study common patterns in alerts, such as types of alerts, geographical locations from where the alerts originated, oldest open alerts, and alerts that took longest time to close.

6.3.3 Filtering Alerts

You can configure alert routing rules to filter the alerts and choose to either store the alerts in the Change Guardian database or drop the filtered alerts.

Change Guardian evaluates the alert routing rules on a first-match basis in top-down order and applies the first matched alert routing rule to alerts that match the filter criteria. If no routing rule matches the alerts, Change Guardian applies the default rule against the alerts. The default routing rule stores all the alerts generated in Change Guardian.

Creating an Alert Routing Rule

To create an alert routing rule to filter the alerts:

1. Log in to the Change Guardian web console.
2. Click **Routing > Alert Routing Rules > Create**.
3. Specify the following information:
   - Name for the alert routing rule
   - Filter criteria
   - Action to take for alerts that match criteria, either store or drop

   WARNING: If you select **Drop**, the filtered alerts are lost permanently.
4. Specify whether you want to enable the alert routing rule at this time.
5. Save the alert routing rule.

Ordering Alert Routing Rules

When there is more than one alert routing rule, you can reorder the alert routing rules by dragging them to a new position or by using the Reorder option. Alert routing rules evaluate alerts in the specified order until a match is made, so you should order the alert routing rules accordingly. Place more narrowly defined alert routing rules and more important alert routing rules at the beginning of the list.

Change Guardian processes the first routing rule that matches the alert based on the criteria. For example, if an alert passes the criteria for two routing rules, only the first rule is applied. The default routing rule always appears at the end.

6.3.4 Configuring Alert Retention Policies

The alert retention policies control when the alerts should be closed and deleted from Change Guardian. If a user does not manually close an alert, it remains open. Alerts notify you of a recent event, so the older an alert is, the less valuable it is. You can configure the alert retention policies to set the duration to automatically close and delete the alerts from Change Guardian.

To configure the alert retention policy:

1. Log in to the Change Guardian web console.
2. Click **Storage > Alert**.

3 Specify the following:

- The number of days from the date of creation of alerts, after which the alert status is set to closed.
- The number of days from the date of closure of alerts, after which the alerts are deleted from Change Guardian.

4 Save the alert retention policy.

7 Understanding Agent Manager

Agent Manager provides services that can manage UNIX and Windows agents, such as:

- Providing a list of computers to which you can deploy agents. This list will be populated by the results of a query against a directory services (Active Directory) or imported from another list.
- Remotely installing Client Agent Manager on a computer that never had any agents. Client Agent Manager receives instructions from Agent Management Services.
- Remotely installing the agent on a computer by using the Client Agent Manager.
- Upgrading an existing agent.

  NOTE: You can roll back the updates.

- Setting configuration of the agents.
- Collecting the installation logs.
- Starting, stopping and restarting agents remotely.

The Agent Manager console provides a central location where you can:

- Manage your agents
- Organise your assets in groups
- Remotely install and update agents on assets

It helps you maintain your environment by keeping track of agents that are not communicating and allows you to either fix the agent or remove it from the environment.

Following are the different attributes in the Agent Manager console:

- **Host Name**: Shows the FQDN of the asset after successful agent deployment.
- **Version**: Shows the Windows version information of the asset after successful agent deployment.
- **Change Guardian Version**: Shows the version of CG Agent installed in target asset(s) after successful agent deployment.
- **Last Communication**: Shows Client Agent Manager last communication time from agent deployed asset to server in Agent Management Service.
- **Modified time**: Shows the modified time of the asset configuration.

7.1 Understanding Asset Groups

An Asset Group is a set of assets or devices that you want to associate with one another. Each Asset Group can contain assets, another Asset Group, or a combination of assets and an Asset Group.

Following are the different types of Asset Groups:

- **All Assets**: All assets added or imported to Agent Manager.

- **Approved Assets**: Assets to which Agent Manager successfully deployed Change Guardian Agent. You do not need to authenticate multiple times for any ‘Install or Upgrade Agents' activity. If the Client Agent Manager service cannot communicate with the Agent Management Service, the asset will move to the “Assets that have not communicated” group.
- **Assets that have not communicated**: Asset from the “Approved asset” group that cannot communicate with Agent Management Service. To move such assets to “Approved asset” group, check if the Client Agent Manager service is communicating with Agent Management Service.
- **Assets not in any group**: Assets that are not part of user-defined group where Agent Manager installed the agent. To categorise the assets from this group to any user defined group, select the asset, go to **Manage Asset** > **Move Assets to a Group** and select the required group.
- **User defined groups**: A list of user defined groups and the categories. To organise and manage assets, you can create your own asset groups under 'User defined groups' section and copy assets from 'Approved Assets' group to user-defined group.

8 Backing Up and Restoring Data

The Change Guardian backup and restore utility is a script that performs a backup of the Change Guardian data and also lets you restore the data at any given point in time.

You can use the backup and restore utility in the following scenarios:

- **System Failure**: In the event of a system failure, you must first reinstall Change Guardian and then use the `cgbackup_util.sh` script with the restore parameter to restore the most recent data that you backed up.
- **Data Loss**: In the event of data loss, use the `cgbackup_util.sh` script with the restore parameter to restore the most recent data that you backed up.

You must back up the following data to make a full restore:

- **Configuration data:** Data stored in the `config`, `data`, `3rdparty/postgresql`, and `3rdparty/jetty` directories, and the data in the Change Guardian database. This data includes configuration files, property files, keystore files, alert rules, all assets and groups in Agent Manager, `.yml` configuration files, Database which stores AMS data, AD Domain information, additional event destination information, email settings, users, filters, and dynamic lists.

  NOTE: The configuration data is critical and you should always include the configuration data in the backup.

- **Event data:** Dynamic event data and raw event data stored in the `data/eventdata` and `/var/opt/novell/sentinel/data/rawdata` directories. The event data also includes event associations stored in the `/var/opt/novell/sentinel/data/eventdata/exported_associations` directory. The event associations data includes correlated event association data and the incident event association data.
- **Secondary storage data:** Closed event data files that have been moved to the secondary storage.
- **Change Guardian logs:** Log files generated by Change Guardian and stored in the `/var/opt/novell/sentinel/log` directory.
- **Change Guardian Policies:** Policies and policy assignments that are stored in Change Guardian server. You can also use the Export and Import options to back up policies. However, backup script allows you to include policies as well in the backed up data.

NOTE: To ensure compatibility, you must restore the data to the same version of Change Guardian that you used to create the backup.

8.1 Parameters for the Backup and Restore Utility Script

The following lists the various command line parameters that you can use with the `cgbackup_util.sh` script:

Table 8-1 *Backup and Restore Script Parameters*

Parameters	Description
-m backup	Backs up the specified data.
-m restore	Restores the specified data. The restore mode of the script is interactive and allows you to specify the data to restore from the backup file. The restore parameter can be used in the following scenarios: ◆ **System Failure:** In the event of a system failure, you must first reinstall Change Guardian and then use the `backup_util.sh` script with the restore parameter to restore the most recent data that backed up. ◆ **Data Loss:** In the event of data loss, use the `backup_util.sh` script with the restore parameter to restore the most recent data that you had backed up. You must restart the Change Guardian server after you restore any data because the script might make several modifications to the database.
-m info	Displays information for the specified backup file.
-m simple_event_backup	Backs up events located in a specified directory.
-m simple_event_restore	Restores events into a specified directory.
-c	Backs up the configuration data, policy editor settings, policies created, and policies assigned.
-e	Backs up the event data. All event partitions are backed up except the current online partition. If the backup is being performed with the Change Guardian server shut down, the current online partition is also included in the backup. It backs up event data from all the directories and subdirectories.
-dN	Backs up the event data for the specified number of days. The -dN option backs up the primary storage event data stored for the last N days. Based on the current data retention policy settings, many days of events might be stored on the system. Backing up all of the event data might not always be necessary and might not be desirable. This option allows you to specify how many days to include when backing up the event data. For example, -d7 includes only the event data from the last week in the backup. -d0 just includes the data for the current day. -d1 includes the data from the current day and previous day. -d2 includes the data from the current day and two days ago. Online backups (that is, backups performed while the system is running) only back up the closed event partitions, which means partitions one day old or older. For online backups, a value of -d1 is the appropriate specification for the number of days.
-u	Specifies the user name to use when backing up the event associations data. If the user name is not specified, "admin" is the default value. This parameter is required only when backing up the event associations data.

Parameters	Description
-p	Specifies the user password when backing up the event associations data. This parameter is required only when backing up the event associations data.
-x	Specifies a file name that contains the user password when backing up the event associations data. This is an alternative to the -p parameter. This parameter is required only when backing up the event associations data.
-f	Specifies the location and name of the backup file.
-l	Includes the log files in the backup. By default, the log files are not backed up unless you specify this option.
-r	Includes the runtime data in the backup. To back up runtime data, you must shut down the Change Guardian server as the data is dynamic. This parameter must be used in combination with the -s option (described below). If -s is not specified, this parameter is ignored.
-b	Backs up the NetFlow data collections and not the entire MongoDB database. The following baseline data is backed up: ◆ configs ◆ anomalydefs ◆ baselines ◆ baselines.ID.URN ◆ paths.UUID.URN ◆ anomalydeployment
-A	Backs up alerts and the events that triggered the alert.
-i	Backs up the entire MongoDB database, NetFlow data collections, and alerts.
-s	Shuts down the Change Guardian server before performing the backup. Shutting down the server is necessary to back up certain dynamic data such as the Runtime data and the current primary storage partitions. By default, the server does not shut down before the backup. If you use this option, the server restarts automatically after the backup is complete.
-w	Backs up the raw event data.
-z	Specifies the location of the event data directory, such as where the event data is collected during a simple_event_backup and where the event data is placed during a simple_event_restore. Only available with the simple_event_backup and simple_event_restore options.

8.2 Running the Backup and Restore Utility Script

You must store the backed up data on a different server. If you use -i or -A options to back up the data, you must restore the configuration data along with alerts. Otherwise, if you restore only alerts data, all the alerts show as remote alerts because the alerts configuration data is not restored.

1 Open a console, and navigate to the `/opt/novell/sentinel/bin` directory as the novell user.

NOTE: By default, the `novell` user does not have a password.

2 Enter `backup_util.sh`, along with the necessary parameters for the data that you want to back up or restore.

For more information on the different parameters, see Table 8-1. The following table lists examples of how to specify the parameters:

Syntax	Action
`cgbackup_util.sh -m backup -c -e -i -l -r -w -s -u admin -x <mypassword.txt> -f /var/opt/novell/sentinel/data/<my_full_backup>.tar.gz`	Shuts down the Change Guardian server and performs a full system backup.
`cgbackup_util.sh -m backup -c -e -i -l -w -u admin -x <mypassword.txt> -f /var/opt/novell/sentinel/data/<my_weekly_backup>.tar.gz`	Performs an online backup without shutting down the server. This backup includes everything except online event data and dynamic runtime data.
`cgbackup_util.sh -m backup -b -c -e -d7 -u admin -x <mypassword.txt> -f /var/opt/novell/sentinel/data/<my_weekly_backup>.tar.gz`	Performs an online backup with event data from the last week. This backup includes configuration data and the event data for the last seven days. Event data older than seven days is not backed up because that data can be extracted selectively, if necessary, from an older backup.
`cgbackup_util.sh -m backup -c -f /var/opt/novell/sentinel/data/config_backup.tar.gz`	Performs a local backup of the configuration data. This is a minimal backup of the system without any event data.
`cgbackup_util.sh -m backup -e -f /var/opt/novell/sentinel/data/events_backup.tar.gz`	Performs a local backup of the event data. This is a minimal backup of the primary storage event data.
`cgbackup_util.sh -m backup -e -d5 -f /var/opt/novell/sentinel/data/events_5days_backup.tar.gz`	Performs a local backup of the event data from the last five days. This is a minimal backup of the primary storage event data from the last five days.
`cgbackup_util.sh -m info -f /var/opt/novell/sentinel/data/config_backup.tar.gz`	Displays the backup information for the specified backup file.

Syntax	Action
`cgbackup_util.sh -m simple_event_backup -e -z /opt/archives/ archive_dir -f /opt/ archives/ archive_backup.tar.gz`	Performs a backup of event data on the computer where the secondary storage directory is located. If the `/opt/archives/archive_dir` is not located in the server, you might need to copy the `backup_util.sh` script to the computer where the secondary storage is located and then run the `simple_event_backup` command from that computer. Alternatively, you can also use any third-party backup tool to back up the event directories on secondary storage.
`cgbackup_util.sh -m restore -f /var/opt/ novell/sentinel/data/ config_backup.tar.gz`	Restores the data from the specified filename.
`cgbackup_util.sh -m simple_event_restore -z /opt/archives/ archivedir -f /opt/ archives/ archive_backup.tar.gz`	Restores the secondary storage data.

3 (Conditional) If you have restored any data, restart the server because the script might make several modifications to the database.

4 Use the Data Restoration feature to restore the extracted partitions. For more information, see Section 8.3, “Restoring Data,” on page 61.

8.3 Restoring Data

The event data restoration feature enables you to restore old or deleted event data. You can also restore the data from other systems. You can select and restore the event partitions in the Change Guardian web interface. You can also control when these restored event partitions expire.

Change Guardian server restarts the services and restores the database after any successful backup and restore.

NOTE: The event data restoration feature is a licensed feature. This feature is not available with the free or trial licenses.

8.3.1 Enabling Event Data for Restoration

To enable event data for restoration, you must copy the event data directories that you want to restore to one of the following locations:

- For primary storage, you can copy the event data directories to `/var/opt/novell/change_guardian/data/eventdata/events/`.

- For secondary storage, you can copy the event data directories to `/var/opt/novell/sentinel/data/archive_remote/<sentinel_server_UUID>/eventdata_archive`.

  To determine the Change Guardian server UUID, perform a search in the web interface. In the Search results, click **All** for any local event.

8.3.2 Viewing Event Data Available for Restoration

1. Log in to the Change Guardian web interface as a user in the administrator role.
2. Click **Storage** > **Configuration**.

   The event data restoration section does not initially display any data.
3. Click **Find Data** to search and display all event data partitions available for restoration.

   The Data Restoration table chronologically lists all the event data that can be restored. The table displays the date of the event data, the name of event directory, and the location. The **Location** column indicates whether the event directory was found in the primary storage directory of Change Guardian or in the configured secondary storage directory.
4. Continue with "Restoring Event Data Where UID and GID are not the Same on the Source and the Destination Server" on page 62 to restore the event data.

8.3.3 Restoring Event Data

1. Select the check box in the **Restore** column next to the partition that you want to restore.

   The **Restore Data** button is enabled when the Data Restoration section is populated with the restorable data.
2. Click **Restore Data** to restore the selected partitions.

   The selected events are moved to the **Restored Data** section. It might take approximately 30 seconds for the **Restored Data** section to reflect the restored event partitions.
3. (Optional) Click **Refresh** to search for more restorable data.
4. To configure the restored event data to expire according to data retention policy, continue with "Restoring Data" on page 61.

Restoring Event Data Where UID and GID are not the Same on the Source and the Destination Server

There may be a scenario where the secondary storage data of the novell user ID (UID) and the group ID (GID) are not the same on both the source (server that has the secondary storage data) and destination (server where the secondary storage data is being restored). In such a scenario, you need to unsquash and squash the squash file system.

To unsquash and squash the file system:

1. Copy the partition that you want to restore on the Change Guardian server where you want to restore the data at the following location:

   `/var/opt/novell/sentinel/data/archive_remote/<sentinel_server_UUID>/eventdata_archive/<partition_ID>`
2. Log in to the Change Guardian server where you want to restore the data, as the `root` user.
3. Change to the directory where you copied the partition that you want to restore:

   `cd /var/opt/novell/sentinel/data/archive_remote/<sentinel_server_UUID>/eventdata_archive/<partition_ID>`

4 Unsquash the `index.sqfs` file:

```
unsquashfs index.sqfs
```

The `index.sqfs` file is unsquashed and the squashfs-root folder is created.

5 Assign permission for novell user and novell group to the <partition_ID> folder:

```
chown -R novell:novell <partition_ID>
```

6 Remove the index:

```
rm -r index.sqfs
```

7 Switch to novell user:

```
su novell
```

8 Squash the `squashfs-root` folder:

```
mksquashfs squashfs-root/ index.sqfs
```

9 Restore the partitions. For more information, see “Restoring Event Data Where UID and GID are not the Same on the Source and the Destination Server”.

8.3.4 Configuring Restored Event Data to Expire

The restored partitions do not expire by default, according to any data retention policy checks. To enable the restored partitions to return to the normal state and also to allow them to expire according to the data retention policy, select **Set to Expire** for data that you want to expire according to the data retention policy, then click **Apply**.

The restored partitions that are set to expire are removed from the Restored Data table and returned to normal processing.

It might take about 30 seconds for the **Restored Data** table to reflect the changes.

9 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 you need to uninstall Change Guardian, contact Technical Support prior to uninstalling the product.

9.1 Change Guardian Upgrade Checklist

Use the following checklist to upgrade your Change Guardian installation. You must upgrade both the Change Guardian server and the Policy Editor. The Windows and UNIX agents are backward compatible.

Table 9-1 *Upgrade Checklist*

	Tasks	See
❒	Ensure that the computers on which you install Change Guardian components meet the specified requirements.	Supported Platforms on the NetIQ web site
❒	If you need to upgrade the operating system on the Change Guardian server, understand the recommended order for the upgrade.	Section 9.2, “Planning an Operating System Upgrade,” on page 66
❒	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 9.3, “Upgrading the Change Guardian Server,” on page 66
❒	Upgrade the Policy Editor.	Section 9.4, “Upgrading Windows-Based Components,” on page 68
❒	(Optional) Upgrade the Windows Agent.	Section 9.4, “Upgrading Windows-Based Components,” on page 68

9.2 Planning an Operating System Upgrade

If the Change Guardian server is running a version of an operating system that is not certified and you need to upgrade the operating system, first upgrade the Change Guardian server and then upgrade the operating system.

If you upgrade the operating system ahead of the Change Guardian server, your existing Change Guardian installation will stop functioning and you will not be able to access the Change Guardian web console until you upgrade the Change Guardian server.

9.3 Upgrading the Change Guardian Server

You can upgrade the following installation types:

- Traditional installation on an existing Linux server
- Appliance installation as a managed software appliance

9.3.1 Upgrading a Traditional Installation

If you are upgrading the Change Guardian Server on a computer running RHEL 6.6, ensure the 64-bit `expect` RPM is installed before you start the upgrade process.

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

To upgrade the Change Guardian server in 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 in the *NetIQ Sentinel Administration Guide*.
2. Download the latest installer from the Patch Finder website. 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 whether 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`

9.3.2 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 more information, see Using Zypper for Interactive Updates and Using WebYaST for Remote Updates.

In some instances, such as an end user license agreement update, you must upgrade the Change Guardian server appliance using Zypper. For information about which methods of upgrade are supported for a release, see the Release Notes.

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 in the *NetIQ Sentinel Administration Guide*.
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 `zypper patch`.

   WARNING: Always use the `zypper patch` command to update/upgrade the Change Guardian appliance. The `zypper up` command is not compatible with the Change Guardian appliance and might cause serious damage to your environment.

   ---
5. (Conditional) If a window asks you to resolve a merge conflict, select **Solution 1**.
6. 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 in the *NetIQ Sentinel Administration Guide*.
4. (Conditional) If you have not already registered the appliance for automatic updates, register for updates. For more information, see Register the Appliance with Customer Center for Updates.

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

Disabling RC4 Communication

In Change Guardian 4.2, the cipher suites are updated to disallow RC4 ciphers. By default, RC4 ciphers were left enabled on all upgraded environments to allow older versions of agents to work with the upgraded CG Server.

Perform the following steps to disable RC4 communication after upgrading:

1. Navigate to `cd /etc/opt/novell/sentinel/3rdparty/jetty`
2. Edit `jetty-ssl.xml`
3. Under the excluded cipher suites section, add the following ciphers:
   - SSL_RSA_WITH_RC4_128_SHA
   - SSL_RSA_WITH_RC4_128_MD5
4. Set the following attributes:
   - **Owner**: Novell
   - **Permissions**: 600
5. Restart services using `/opt/netiq/cg/scripts/cg_services.sh restart` command.

Using Zypper for Interactive Updates

Use Zypper to perform interactive updates on the appliance.

1. Log in to the appliance as `root`.
2. Run the following command: `zypper patch`

   WARNING: Always use the zypper patch command to update/upgrade the Change Guardian appliance. The zypper up command is not compatible with the Change Guardian appliance and might cause serious damage to your environment.
3. Restart the appliance.

For more information, see the Zypper Cheat Sheet.

Using WebYaST for Remote Updates

Use WebYaST to manage appliance updates from a web-based remote console. You can access WebYast in the following ways:

- Through the Change Guardian web console appliance dialog
- Directly at https://IP_Address_Change_Guardian_Server:54984

For more information, see the WebYaST documentation.

9.4 Upgrading Windows-Based Components

The procedures for upgrading the Policy Editor and the Windows agent are the same as the procedures for installing them, except that you do not need to repeat the process of adding assets to Agent Manager. For more information, see Section 3.2, “Installing the Policy Editor,” on page 27 and Section 3.3, “Installing the Windows Agent,” on page 28.

10 Uninstalling 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 you need to uninstall Change Guardian, contact Technical Support prior to uninstalling the product.

10.1 Change Guardian Uninstallation Checklist

Use the following checklist to uninstall your Change Guardian installation:

- Uninstall the Change Guardian server
- Uninstall the Policy Editor
- Uninstall the Windows Agent
- Perform post-uninstallation tasks to complete the Change Guardian uninstallation

10.2 Uninstalling the Change Guardian Server

To uninstall the Change Guardian server:

1. Log in to the Change Guardian server as root.

   NOTE: You must use the same user account to uninstall the Change Guardian server you used to install it. For example, a non-root user, can uninstall the Change Guardian server if a non-root user performed the installation.

2. Access the following directory: `/opt/novell/sentinel/setup/`
3. Run the following command: `./uninstall-changeguardian`
4. When prompted to reconfirm that you want to proceed with the uninstall, press **y**. The script first stops the service and then removes it completely.

10.3 Uninstalling the Windows Agent

Use the following steps to uninstall the Windows Agent:

1. Go to **Control Panel** > **Programs and Features:** and search for Change Guardian Windows Agent.
2. Select the Change Guardian Windows Agent application, then click **Uninstall**.

10.4 Uninstalling Policy Editor

Use the following steps to uninstall the Policy Editor:

1. Go to **Control Panel** > **Programs and Features:** and search for Change Guardian Policy Editor.
2. Select the Change Guardian Policy Editor application, then click **Uninstall**.

10.5 Post-Uninstallation Tasks

After you uninstall Change Guardian:

- Reboot the computer to clear the cache files
- To ensure that the novell, sentinel, java and javos services are not running, run the following command

```
ps -ef | grep novell
ps -ef | grep Sentinel
ps -ef | grep java
ps -ef | grep javos
```

NOTE: If the services are still running, the re-installation of the Change Guardian server fails with errors or exceptions.

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)

The following table lists the requirements and recommendations for computers running Active Directory Domain Services:

Category	Requirement
Operating System	One of the following: ◆ Windows Server 2012 R2 ◆ Windows Server 2012 ◆ Windows Server 2008 R2 ◆ Windows Server 2008 (32- and 64-bit) ◆ Windows Server 2003 R2 (32- and 64-bit)

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 in 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 then 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 in 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 User and Group Auditing

This configuration enables auditing of user logons and logoffs (by both local users and Active Directory users) and local user and group settings.

You can configure user and group auditing manually or by running scripts.

A.3.1 Configuring Manually

To manually configure user and group auditing, complete the following steps.

To manually configure user and group auditing:

1. Log in to a computer in the domain you want to configure using a user account with domain administrator privileges.
2. Open the Microsoft Management Console, and then select **File > Add/Remove Snap-in**.
3. Select **Group Policy Management Editor**, and then click **Add**.
4. On the Select Group Policy Object window, click **Browse**.
5. Select **Domain Controllers.*FQDN***, where *FQDN* is the Fully Qualified Domain Name for the domain controller computer.
6. Click **Add**.
7. Select **Default Domain Controllers Policy**, and then click **OK**.
8. Click **Finish**, and then click **OK**.
9. In the Microsoft Management Console, expand **Default Domain Controllers Policy *FQDN* > Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Audit Policy**.
10. Under **Audit Account Logon Events**, select **Define these policy settings**, and then select **Success** and **Failure**.
11. Under **Audit Logon Events**, select **Define these policy settings**, and then select **Success** and **Failure**.

12 In the Microsoft Management Console, expand **Default Domain Controllers Policy *FQDN* > Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies > Logon/Logoff**.

13 Under **Audit Logon**, select **Audit Logon**, and then select **Success** and **Failure**.

14 Under **Audit Logoff**, select **Audit Logoff**, and then select **Success** and **Failure**.

15 To update Group Policy settings, open a command prompt and type `gpupdate /force`.

A.3.2 Configuring with Scripts

The following scripts enable user and group auditing:

- **ADLogonEventConfig.vbs -** audits logon/logoff activity for Active Directory users logged on to the domain controller computer in your Change Guardian environment
- **CGWAuditingConfig.vbs -** audits local user and group settings and logon/logoff activity for local users
- **ADPrereqConfig.vbs -** audits Active Directory event generation

The scripts are part of the agent installation and are available in the Change Guardian installation directory on the agent computer (typically `c:\Program Files\NetIQ\ChangeGuardianAgent\`).

To run the scripts, open a command prompt and use the following syntax:

```
cscript.exe 'Script Name'
```

You can run the scripts in any order.

A.4 Configuring Active Directory Security Access Control Lists

The Security Access Control List (SACL) describes the objects and operations to monitor. You must configure the SACL 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.4.1, “Configuring SACLs for Change Guardian for Active Directory,” on page 74. If you are running only Change Guardian for Group Policy in your environment, see Section A.4.2, “Configuring SACLs for Change Guardian for Group Policy Only,” on page 76.

A.4.1 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.

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.

To verify or set this configuration:

1. Log in 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 that **Name** is set to `Default naming context`, and **Path** points to the domain to configure.

   NOTE: You must perform Step 5 through Step 13 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 list.
   - 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 Step 5 through Step 13 two more times.

A.4.2 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 in 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** > **Auditing** > **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:
    - 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

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 In **Connection Point**, select **Select a well known Naming Context**, and then select **Configuration** in the drop-down list.

15 Click **OK**, and then expand **Configuration**.

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

17 Select the **Security** tab.

18 Click **Advanced**.

19 Click **Auditing**.

20 Click **Add**.

21 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

22 In the **Applies to** or **Apply onto** field, select **This object and all descendant objects**.

23 Clear the setting to **Apply these auditing entries to objects and/or containers within this container only**.

24 Click **OK** until you close all open windows.

A.5 Synchronizing Active Directory User Accounts

Synchronizing Active Directory user accounts allows you to retrieve information about the user associated with a particular event, such as the user name, the user's email address, and the user's contact details. The user information comes from the Active Directory server in your environment. You can also view all the user's recent activities.

Using the Change Guardian web console, you add one or more user containers and the user attributes that you want to synchronize.

To view and manage synchronized Active Directory accounts:

1 In the Change Guardian web console, click **Integration**.

2 Click **AD Accounts**.

A.5.1 Adding a User Container

Active Directory stores user accounts in containers. You can add one or more containers to Change Guardian to synchronize the users accounts.

To add a user container to Change Guardian:

1 In the Change Guardian web console, click **Integration > AD Accounts > Add User Container**.

2 Provide the appropriate information for the user container you want to synchronize.

A.5.2 Mapping User Profile Fields

To synchronize Active Directory user accounts to Change Guardian, Change Guardian needs to map the user account field names in Active Directory to an attribute in your directory service. By default, Change Guardian maps the most commonly used field names, but you can add or remove mappings as necessary.

To modify user profile mapping, in the Change Guardian web console, click **Integration > AD Accounts > User Profile Mapping**.