Change Guardian™

Installation and Administration Guide

December 2019

NetIQ

Legal Notice

Contents

About this Book and the Library

The *Installation and Administration Guide* provides instructions about installing and upgrading Change Guardian. This book also includes guidance for initial configuration to get you started.

Intended Audience

This book provides information for administrators who are responsible for installing and administering Change Guardian.

Additional Documentation

The Change Guardian documentation library includes the following resources:

User Guide

Provides information about the tasks that can be performed by a Change Guardian user who analyzes the change events.

Release Notes

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

1 Introduction

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)

This section provides information about the following:

- "What is Change Guardian?" on page 11
- "How Change Guardian Works" on page 12

What is Change Guardian?

Change Guardian provides security intelligence to rapidly identify and respond to privileged-user activities if the activity signals a security breach or it results in compliance gaps. Change Guardian helps security teams detect and respond to potential threats in real-time by using intelligent alerting of authorized and unauthorized access, and helps detect changes to critical files, systems, and applications.

To manage sophisticated threats and complex computing environment, 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 about 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, and enable a fast 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 different platform logs in the following ways:

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

Change Guardian also integrates with your existing security information and event management (SIEM) solution, such as 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 can mitigate the impact of an attack before serious damage or compliance gaps can occur.

How Change Guardian Works

Change Guardian collects events from assets using Change Guardian agents. For example, when a Windows machine logs an event such as, file property changed, file created, user permission changed, user logged in, Change Guardian Agent for Windows collects the event data. The event data contains who, what, when, and where.

Agents collect events based on rules set by Change Guardian policies. A policy defines what type of events are to be collected, assign risk value to an event, assign specific users to allow the change, set event severity, and so on. When an agent collects events, Change Guardian can notify you through pre-configured emails or alerts in the dashboard.

Change Guardian provides the following interfaces to view events and take action:

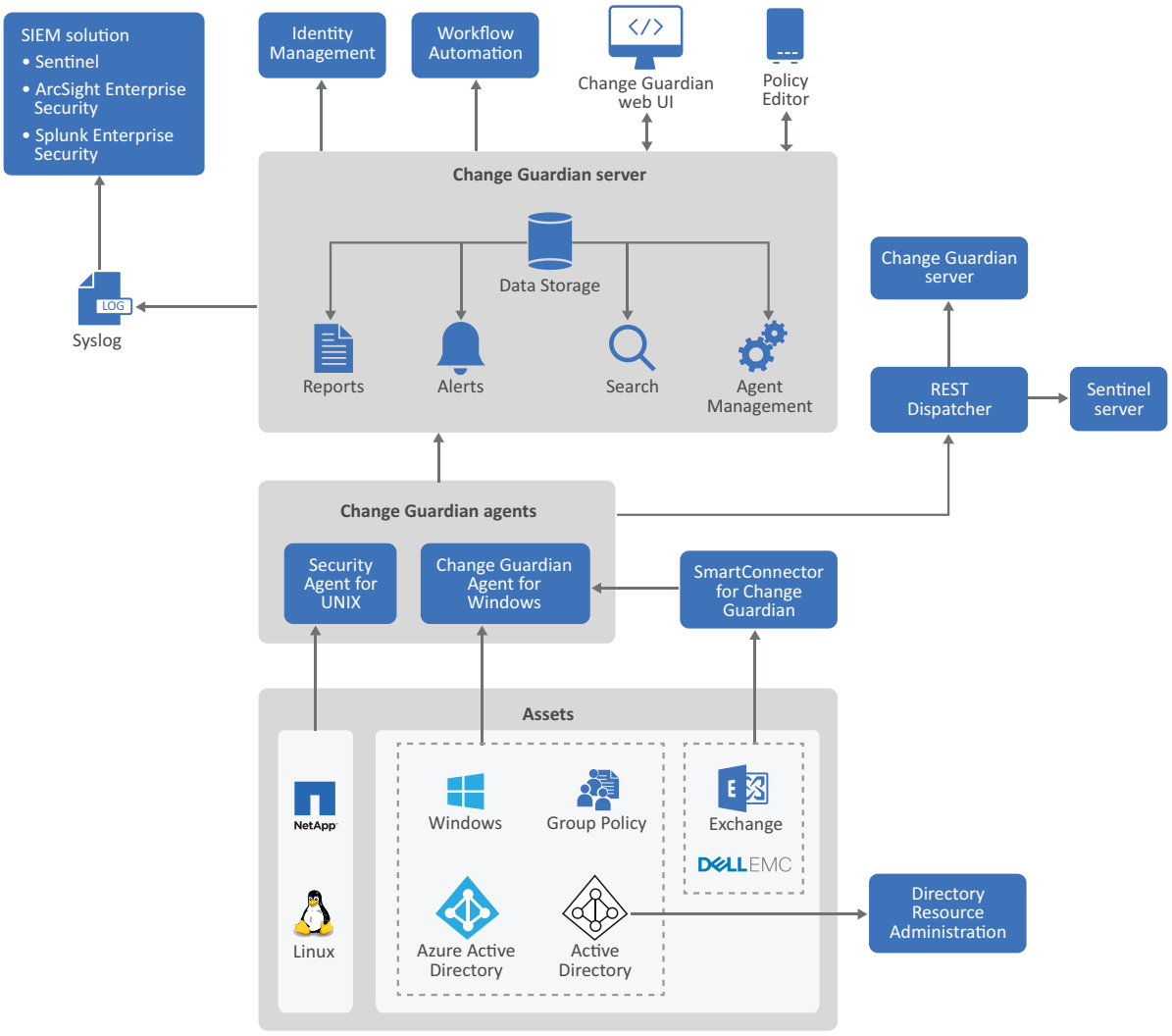
Change Guardian dashboards: Allows you to view all events and manage alerts created using Change Guardian.

Administration Console: Allows you to view and interact with data collected by Change Guardian.

Change Guardian events can be forwarded to other softwares for further analysis, and for long term retention such as another Change Guardian server, Sentinel server, or Splunk Enterprise Security. Change Guardian works with Directory Resource Administrator and Identity Manager track identities of users accounts.

Change Guardian Architecture

The following diagram illustrates how Change Guardian works:



Components in the Diagram	Description
Assets	Endpoints from where Change Guardian agents collect events.
Change Guardian Agents	Windows or UNIX based software that collects event data from the assets and forwards them to the Change Guardian server.
SmartConnector for Change Guardian	Collects event data in Common Event Format (CEF) from Dell EMC and Microsoft Exchange, and forwards to Change Guardian Agent for Windows.

Components in the Diagram	Description
Change Guardian Server	A Linux-based computer that receives and stores the event data. The server also stores the policies that you create. The server provides the capabilities of searching events and creating alerts and reports.
Agent Management	A central location where you can manage agents. Agent Manager allows you to deploy and manage your agents directly on the agent host machine, or remotely install agents.
Policy Editor	A Windows-based console where you create as well as deploy policies and alerts for asset monitoring.
Change Guardian Web UI	Interfaces to dashboards and management consoles where you can view events, view and triage alerts, create event and alert routing rule, manage users, and so on.

2 Planning the Installation

This section provides information on how to plan your Change Guardian server installing.

Implementation Checklist

Review the following table before you begin installing Change Guardian:

	Checklist Item	See
❑	Review the Change Guardian architecture that is suitable for your environment.	(Optional) Consulting Services
❑	Ensure that you have the following license keys: ◆ Change Guardian server ◆ Change Guardian Module Keys ◆ NCC channel registration codes (only for appliance installations)	“Understanding Licensing” on page 15
❑	Determine whether you want to perform a traditional or appliance installation of the Change Guardian server.	“Installation Options” on page 20
❑	Identify the modules that you want to monitor.	“Configuring Event Monitoring” on page 59
❑	Review the recommended hardware, supported operating systems versions, appliance platforms, and browsers requirements.	Change Guardian 5.2 System Requirements
❑	Review the latest Change Guardian release notes to understand the new functionality and the known issues.	Change Guardian 5.2 Release Notes

Understanding Licensing

Change Guardian comprises of a broad spectrum of functionalities which cater to various needs of its many customers. The three types of licenses for Change Guardian are as follows:

- At least one Change Guardian server.
- **A licensed count of monitored application.** The following is the list of applications:
  - Windows Server: Number of monitored Microsoft Windows Server Class logical operating system instances.

- Windows Workstation: Number of monitored Microsoft Windows Workstation Class logical operating system instances.
- Active Directory and Group Policy: Number of enabled Active Directory User module.
- UNIX Server: Number of monitored UNIX, Linux, or UNIX-derivative Server Class logical operating system instances.
- UNIX Workstation: Number of monitored UNIX, Linux, or UNIX-derivative Workstation Class logical operating system instances.
- Microsoft Azure Active Directory: Number of enabled Microsoft Azure Active Directory User modules.
- NetApp Share: Number of enabled user modules.
- Microsoft Exchange Server
- Dell EMC

NOTE: For more information on managing applications and their licenses, see:

- “Installing Change Guardian Components” on page 31
- “Adding License for Modules or Applications” on page 45

- Registration code to download appliance updates. (applicable only for appliance installations)

NOTE: New Change Guardian installations are set up with a default evaluation key for the server and all modules, which you can use until you apply your official customer keys. All three types of license keys are available from the Customer Care Portal.

The following sections provide information about the types of Change Guardian licenses.

- “Evaluation Licenses” on page 16
- “Enterprise Licenses” on page 16
- “Module or Application Licenses” on page 17

Evaluation Licenses

If you have not yet purchased Change Guardian, you may use the 60-day built-in trial license. Contact your Sales Associate for further assistance.

The default evaluation license allows you to use all the features of Change Guardian during the evaluation period.

By default, new installations of Change Guardian server include evaluation licenses for all modules.

The expiration date of the system is based on the oldest data in the system. If you restore old events to your system, Change Guardian updates the expiration date accordingly.

To prevent any interruption in functionality, you must upgrade the system with an enterprise license before the evaluation license expires.

Enterprise Licenses

When you purchase Change Guardian, you receive the license keys and registration codes through the customer portal, including the following:

- HTML license key for the Change Guardian server

- XML license keys for each licensed module (such as Active Directory or NetApp Share)
- (optional) Alphanumeric registration code to register your Change Guardian appliance for the appliance update channel

You can use the same registration code for the old appliance update channel (for appliances prior to 5.1) and the new appliance update channel (for 5.1 and later appliances).

There might be additional license terms that are not enforced by the license key, therefore read your license agreement carefully.

To make changes to your licensing, contact your account manager.

You can add the enterprise license key either during the installation or any time thereafter.

Module or Application Licenses

You require an application license to enable Change Guardian to monitor that application. Licenses are available for the following applications:

- Windows Active Directory
- Microsoft Azure Active Directory
- Dell EMC
- Microsoft Exchange
- Group Policy
- NetApp
- Linux and UNIX
- Windows

Understanding Ports Used

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

Component	Ports	Direction	Required /Optional	Description
Policy Editor Console	TCP 8443	Outbound	Required	Connects to the Change Guardian server for the following actions: ◆ configuring email in Change Guardian or Sentinel ◆ updating policies to the Change Guardian server
	TCP 2620	Outbound	Optional	Allows remote object browsing to UNIX-based monitored assets.
	TCP 389 or TCP 636	Outbound	Optional	Allows remote object browsing to Active Directory.
	TCP 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.

Component	Ports	Direction	Required /Optional	Description
Change Guardian Server	TCP 389 or TCP 636	Outbound	Required	Enables the LDAP authentication and the expansion of Active Directory groups. The port initiates a connection to the LDAP server.
	TCP 25	Outbound	Optional	Default email port. This port may be different based on the specific email implementation.
	TCP 1099 and 2000	Inbound	Required	Used together by monitoring tools to connect to Change Guardian server process using Java Management Extensions (JMX).
	TCP 5432	Inbound	Optional. By default, this port listens only on loopback interface.	Used for the PostgreSQL database.
	TCP 137, 138, 139, 445	Outbound	Optional	If secondary storage is configured to use CIFS.
	TCP/UDP 111 and TCP/UDP 2049	Outbound	Optional	If secondary storage is configured to use NFS.
	UDP 514 or TCP 1468	Outbound	Optional	This port is used when Change Guardian forwards events to the system receiving Syslog messages. If the port is UDP, it sends a packet to the receiver. If the port is TCP, it initiates a connection to the receiver.
	TCP 27017			Used for the Security Intelligence configuration database.
	TCP 28017			Used for the web console for Security Intelligence database.
	TCP 32000			Used for internal communication between the wrapper process and the server process.
	TCP 9200			Used for communication with alert indexing service using REST.
	TCP 9300			Used for communication with alert indexing service using its native protocol.
	TCP 443	Inbound	Optional	Forwarded to 8443 for HTTPS communication.
	TCP 61616	Inbound	Optional	Used for incoming connections from Sentinel Collector Managers.
	TCP 9443	Inbound	Required	Used by the Change Guardian Appliance Management Console.

Component	Ports	Direction	Required /Optional	Description
JAVOS	TCP 8094	inbound	Required	Allows the JAVOS service to accept connections from agents that are retrieving their assigned monitoring policies.
	TCP 9094	Inbound (loopback)	Required	Allows the Change Guardian server to call JAVOS on this port to signal/reset the event destination cache.
	TCP 9095	Inbound (loopback)	Optional	Allows users to see runtime metrics and active threads.
Active Directory Accounts/ LDAP Expander	TCP 8088	Inbound (loopback)	Required	Allows the Change Guardian server to retrieve information about Active Directory accounts.
	TCP 8089	Inbound (loopback)	Optional	Allows users to see runtime metrics and active threads.
Windows Monitoring Agents	TCP 8094	Outbound	Required	Allows the agent to connect to the Change Guardian server to retrieve assigned monitoring policies.
	TCP 8094	Inbound	Optional	Allows the Policy Editor to connect to the agent to browse objects on the monitored asset.
	TCP 8443	Outbound	Required	Allows the agent to connect to the Change Guardian server or Sentinel to send events.
UNIX Monitoring Agents	TCP 8094	Outbound	Required	Allows the agent to connect to the Change Guardian server to retrieve assigned monitoring policies.
	TCP 2620	Inbound	Optional	Allows the Policy Editor to connect to the agent to browse objects on the monitored asset.
	TCP 8443	Outbound	Required	Allows the agent to connect to the Change Guardian server or Sentinel to send events.
UNIX Agent Manager	TCP 2620	Outbound	Required	Allows the UNIX Agent Manager to connect to a UNIX agent to get status and diagnostic information.
	TCP 2222	Outbound	Required	Allows the UNIX Agent Manager client to connect with the UNIX Agent Manager server.
	TCP 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.
	TCP 21/23	Outbound		(Telnet/FTP) UNIX Agent Manager requires SSH+SFTP or Telnet+FTP access to computers targeted for remote agent deployment.
Agent Manager	TCP 8082	Inbound	Required	Allows the agent to communicate with the Agent Manager.
	TCP 445	Outbound	Required	Allows the Agent Manager to deploy agents to Windows computers.
	TCP 22	Outbound	Required	Allows the Agent Manager to deploy agents to Windows computers.

Installation Options

Use this section to determine the installation option that suits your environment.

Traditional Installation

This form of installation provides the following:

- The flexibility to select the operating system vendor of your choice
- The flexibility to manage your own licenses and patch updates
- The flexibility to set firewall yourself
- More customization options for product configuration during installation

Appliance Installation

This form of installation provides the following:

- A Change Guardian server appliance that is a ready-to-run software appliance built on SUSE Studio
- An integrated update service for both product and the operating system that are available by Micro Focus
- Preconfigured firewall
- A web interface to configure and manage the appliance and receive the patch updates

Security Considerations

Following sections provide information about the security considerations before installing Change Guardian.

- “Traditional Installation” on page 20
- “Appliance Installation” on page 21
- “Using TLS for Communication” on page 21

Traditional Installation

- The administrator should close all unnecessary ports. For more information, see “Understanding Ports Used” on page 17.
- Service port listens preferably only for local connections, and does not allow remote connections.
- Files are installed with least privileges so that the least number of users can read the files.
- Reports against the database are run as a user that only has SELECT permissions on the database.
- All web interfaces require HTTPS protocol.
- All communication over the network uses SSL by default and is configured to require authentication.
- User account passwords are encrypted by default when they are stored on the file system or in the database.

Appliance Installation

The appliance has undergone the following hardening:

- Only the minimally required packages are installed.
- The firewall is enabled by default and all unnecessary ports are closed in the firewall configuration.
- Change Guardian is automatically configured to monitor the local operating systems syslog messages for audit purposes.

Using TLS for Communication

The TLS 1.0 communication protocol has known vulnerabilities. You must use TLS 1.1 or later for communication.

TLS 1.0 is disabled by default in new installations of the Change Guardian server, agents, and Policy Editor components to improve security posture and to prevent known vulnerabilities.

3 Installing Change Guardian

This chapter guides you through installing the Change Guardian server and its components.

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 “How Change Guardian Works” on page 12.

Installation Checklist

Use the following checklist to plan, install, and configure Change Guardian.

If you are upgrading from a previous version of Change Guardian, do not use this checklist. For information about upgrading, see Chapter 13, “Upgrading Change Guardian,” on page 139.

	Checklist Item	See
❑	Install Change Guardian.	“Traditional Installation” on page 23 “Appliance Installation” on page 29
❑	Install the Change Guardian components.	“Installing Change Guardian Components” on page 31
❑	Configure the server.	“Configuring Change Guardian” on page 36
❑	(Conditional) If you change the IP address of the Change Guardian server, there is a break down of communication between the server and agent. This requires reconfiguration of the server to restore communication. Therefore, it is recommended to use static IP addresses in your Change Guardian deployment.	-

Traditional Installation

IMPORTANT: You cannot install Change Guardian server as a non-root user.

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 “Configuring FIPS 140-2” on page 37.

NOTE: FIPS mode is supported only for Change Guardian. Change Guardian is not supported if the operating system is in FIPS mode.

Prerequisites

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

- bash
- bc
- curl
- expect
- coreutils
- gettext
- glibc
- grep
- libgcc
- libstdc
- lsof
- net-tools
- openssl
- python-libs
- samba-client
- samba-common-libs
- samba-common-tools
- samba-libs
- sed
- tcl
- zlib
- fontconfig
- dejavu-fonts

NOTE: For SLES 11 SP4 platform, enable SLES 11-Security-Module to install the `curl-openssl1` package before installing Change Guardian.

Performing an Interactive Installation

This section provides information about standard and custom installation.

Standard Installation

Use the following steps to perform a standard installation:

To install the Change Guardian server:

1. On the command line, log in as the root user and 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 as the root user by typing the following command in the root of the extracted directory:

   `./install-changeguardian.sh`

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

   Or

   If you want to install Change Guardian on more than one system, you can record your installation options in a file. You can use this file for an unattended Change Guardian installation on other systems. To record your installation options, specify the following command: `./install-sentinel -r <response_filename>`

3. Specify the language as English, then press Enter. The end user license agreement is displayed in the selected language.

4. Press the space bar to read the license agreement. You must scroll through the entire agreement before you can accept it.

5. When prompted, select the standard configuration.

   The 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.

6. Create an admin account password for global system administration.

   NOTE: While setting the admin password, only the following non-alphanumeric characters are allowed:` ! @ $ ^ _ { } [ ] \ : " , . / ?.

   ---

7. 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.

   ---

8. 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. For secure connection use 587.
- **From** – The return email address appearing on each email sent.
- **SMTP User Name (Optional)** – The user name to connect to the SMTP server.
- **SMTP Password (Optional)** – The password that corresponds to the SMTP user name.
- **Secure Connection** – The connection mechanism for STARTTLS protocol.

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_cg.sh` script to update this configuration. For more information, see "Changing Default Email Host Settings" on page 39.

8a (Conditional) If the SMTP server certificate is self-signed, or if not signed by a well-known CA, such as VeriSign, you have to import the certificate to the server's trust-store. To import the self-signed certificate or CA certificate, complete the following steps:

8a1 Download the certificate to the server.

8a2 To store the certificate in `activemqkeystore`, run the following command at the server machine: `/opt/novell/sentinel/jdk/jre/bin/keytool -import -alias <appropriate_alias> -keystore /etc/opt/novell/sentinel/config/.activemqkeystore.jks -file <certificate_file_path> -storepass password`

8a3 Restart the server by running the following command: `rcsentinel restart.`

After the Change Guardian server installation completes, 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.

Custom Installation

Use the following steps to perform a custom installation.

To install the Change Guardian server:

1. On the command line, log in as the root user and type the following command to extract the installation file:

   `tar zxvf cgserver-x.x.x-xx.x86_64.tgz`

2. To install from a custom path, specify the following command: `./install-changeguardian.sh --location=<custom_CG_directory_path>`

   NOTE: This custom path must have 0755 permissions.

   Or

   If you want to install Change Guardian on more than one system, you can record your installation options in a file. You can use this file for an unattended Change Guardian installation on other systems. To record your installation options, specify the following command: `./install-sentinel --location=<custom_CG_directory_path> -r <response_filename>`

3. Specify the language as English, then press Enter. The end user license agreement is displayed in the selected language.
4. Press the space bar to read the license agreement. You must scroll through the entire agreement before you can accept it.

NOTE: The installation finishes with the message: “Change Guardian installation is complete”.

5 When prompted, select custom configuration, and complete the configuration by 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 currently not supported. For more information about configuring Change Guardian to run in FIPS mode, see “Configuring FIPS 140-2” on page 37.

NOTE: While setting the admin password, only the following non-alphanumeric characters are allowed:` ! @ $ ^ _ { } [ ] \ : " , . / ?.

6 Create an admin account password for global system administration.

7 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.

8 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. For secure connection use 587.
- **From** – The return email address appearing on each email sent.
- **SMTP User Name (Optional)** – The user name to connect to the SMTP server.
- **SMTP Password (Optional)** – The password that corresponds to the SMTP user name.
- **Secure Connection** – The connection mechanism for STARTTLS protocol. Set the value to `true` if you want to configure SMTP server for STARTTLS.

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_cg.sh` script to update this configuration.

8a (Conditional) If the SMTP server certificate is self-signed or not signed by a well-known CA, such as VeriSign, you have to import the certificate to the server's trust-store. To import self-signed certificate or the CA certificate, complete the following steps:

8a1 Download the certificate to the server.

8a2 To store the certificate in `activemqkeystore`, run the following command at the server machine: `/opt/novell/sentinel/jdk/jre/bin/keytool -import -alias <appropriate_alias> -keystore /etc/opt/novell/sentinel/config/.activemqkeystore.jks -file <certificate_file_path> -storepass password`

8a3 Restart the server by running the following command: `rcsentinel restart.`

After the Change Guardian server installation completes, 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.

Performing a Silent Installation

The silent or unattended installation is useful if you need to install more than one Change Guardian in your deployment. You can record the installation parameters during the interactive installation and then run the recorded files on other systems.

Ensure that you have recorded the installation parameters to a file. For more information about creating the response file, see:

- Standard Installation
- Custom Installation

To enable FIPS 140-2 mode, ensure that the response file includes the following parameters:

- ENABLE_FIPS_MODE
- NSS_DB_PASSWORD

To perform a silent installation:

1. Download the installation files from the Download site.
2. Log in as `root` to the server where you want to install Change Guardian.
3. Specify the following command to extract the install files from the tar file: `tar -zxvf <install_filename>`
4. To record the steps to a response file, run the following command: `./install-sentinel -u <response_filename>`

   The installation proceeds with the values stored in the response file. Wait until the installation finishes before you log in to the server.

Appliance Installation

The Change Guardian server appliance is a ready-to-run software appliance. 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.

To install the Change Guardian Server appliance image:

1. Download the base appliance image to a local server from the Change Guardian 5.2 downloads page. The OVF file name is `ChangeGuardian_SLES12SP3GM_5.1.0.0.x86_64-5064.3.1.ovf.tar.gz`. The ISO file name is `ChangeGuardian_SLES12SP3GM_5.1.0.0.x86_64-5064.3.1.preload.iso`.

   IMPORTANT: To create a new instance of Change Guardian 5.2 appliance, you must first install the Change Guardian 5.1 appliance base image and then apply the latest product and operating system updates from the appliance channel.

2. (Conditional) If you are using VMware, 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 <filename>`
   - **2b** For VMware, log in to the vSphere client and deploy the OVF template. For more information, see the VMware documentation.
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 SUSE End User License Agreement.
7. Read and accept the 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

NOTE: While setting the admin password, only the following non-alphanumeric characters are allowed:` ! @ $ ^ _ { } [ ] \ : " , . / ?.

- 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.

12 Download the following file to the Change Guardian server: `changeguardian_appliance_configuration_utility_5100-32.tar.gz` from Micro Focus Downloads.

13 Extract the file by running the following command: `tar -xvf changeguardian_appliance_configuration_utility_5100-32.tar.gz`.

14 Use the `cd` command to change to the directory where you extracted the utility.

15 To configure the appliance, run the following script:

```
./cg5100-appliance_configuration.sh
```

This script configures the required packages to manage the appliance.

WARNING: Do not run this script remotely as it involves network reconfiguration, which in turn might interrupt the configuration.

---

16 Register your appliance for updates to receive updates for the appliance.

17 To complete the appliance installation, apply the latest product and operating system updates from channel. For more information on applying updates, see “Applying the Updates” on page 143.

Registering the Appliance for Updates

You must register the Change Guardian appliance with the appliance update channel to receive Change Guardian and latest operating system updates. To register the appliance, you must first obtain your appliance registration code or the appliance activation key from the Customer Care Center.

- "Register Using Change Guardian Appliance Management Console" on page 31
- "Register Using Commands" on page 31

Register Using Change Guardian Appliance Management Console

Use the following steps to register the appliance for updates:

1. Log in to the Change Guardian Appliance Management Console as vaadmin or root.
2. Click **Home > Online Update > Register Now**
3. In the **Email** field, specify the email ID to which you want to receive updates.
4. In the **Activation Key** field, enter the registration code.
5. Click **Register**
6. Verify whether updates are available.

Register Using Commands

Use the following steps to register the appliance for updates:

1. Log in to the Change Guardian server as the root user.
2. Clean up existing registrations.
   - For SLES (both 11 and 12) based clients, run the following command as root user:

     ```
     suse_register -E
     ```
3. Specify the following command to register the server:
   - For SLES (both 11 and 12) based clients, run the following command as root user:

     ```
     suse_register -a regcode-change-guardian="<registration_code>" -a
     email="<email_ID>"
     ```

   Specify the email ID where you want to receive updates.

   SLES OS updates are also provided through the appliance update channel.
4. Verify whether updates are available.

   For more information on applying updates, see "Applying the Updates" on page 143.

Installing Change Guardian Components

You have to install the following Change Guardian components:

For information about requirements and recommendations for computers running the Policy Editor, see the Technical Information for Change Guardian 5.2 page.

Policy Editor The interface allows you to configure policies and assign policies to assets that you want to monitor. The assets that Change Guardian monitors are Microsoft Active Directory (AD), Microsoft Azure AD, Dell EMC, Microsoft Exchange, Group Policy, NetApp, Linux and UNIX, and Windows.

Change Guardian Agent for Windows Collects change event data for Windows, Windows Active Directory, Microsoft Azure Active Directory, Microsoft Exchange, Group Policy, and Dell EMC.

Security Agent for UNIX Collects change event data for Linux, UNIX, and NetApp.

SmartConnector for Change Guardian Collects change event data in Common Event Format (CEF) from Dell EMC and Microsoft Exchange.

If you want to install a custom configuration not identified in the sections that follow, or if you have questions, contact Technical Support.

IMPORTANT: You can install the Change Guardian components only as an administrator.

Installing Policy Editor

To install Policy Editor, complete the following steps.

To install the Policy Editor:

1. From Administration Console click, **Integration** > **Agent Manager**.
2. Click **All Assets**, and then click **Manage Installation** and select **Download**.
3. Select **Change Guardian Policy Editor**, and then click **Start Download**.

   Agent Manager downloads `ChangeGuardianPolicyEditor.zip` to your computer.
4. 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.
5. Log in to the computer where you want to install the Policy Editor with an administrator account.
6. Run the installation program, `NetIQCGPolicyEditorInstaller.exe`, and follow the instructions.
7. When the installation completes, click **Finish**.

Accessing 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.

NOTE: You must always launch Policy Editor with an account in the local Administrators group.

Installing Change Guardian Agent for Windows

You can install Change Guardian Agent for Windows in the following ways:

- Install agents remotely using the Agent Manager
- Install the agent manually on a local computer

NOTE: Agent Manager and the Change Guardian Agent for Windows are in FIPS mode by default.

Following sections provide information about installing Change Guardian Agent for Windows.

- "Remote Installation" on page 33
- "Manual Installation" on page 34

Remote Installation

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

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 and install the agents.

To install Change Guardian Agent for Windows using Agent Manager:

1. From Administration Console, click **Integration** > **Agent Manager**.
2. From the assets list, select the computers where you want to deploy the agent. If you select multiple computers, they must use the same credentials.

   For more information, see "Adding Assets" on page 43
3. Click **Manage Installation**, and then select **Install**.
4. In case of a newly added asset, log in as `root`, to the computer that you want to connect to and click **Next**.

   NOTE: You must be logged in as an administrator to deploy agents. The account must be the local administrator account or a domain account in the Local Administrators group.

   ---
5. For the agent version, select **Change Guardian Agent for Windows *Version***.
6. For the agent configuration, you can choose the default configuration. If you want to modify the default configuration, use the **Edit** option to customize the default configuration.
7. Otherwise, if required, you can add a new configuration using the **Add** option.
8. Click **Start Installation**

Agent Manager initiates the action that you selected. Use the **In progress Tasks**, **Completed Tasks**, and **Failed Tasks** tabs to monitor the progress.

NOTE: When you use the Agent Manager to install Change Guardian Agent for Windows, Agent Manager communicates with the agent through the Agent Management service.

To reconfigure an agent using Agent Manager:

1. Ensure that you have completed the steps in section "Adding Assets" on page 43.

2 From the assets list, select the computer where you want to deploy an agent.

3 Provide credentials for an account that can connect to the computer and click **Next**.

The account must be the local administrator account or a domain account in the Local Administrators group.

4 Click **Manage Installation**, and then select **Reconfigure**.

5 Perform the following steps:

5a For the agent version, select **Change Guardian Agent for Windows *Agent Version***, where *Agent Version* is the version of the Change Guardian Agent for Windows you want to deploy.

5b For the agent configuration, click add a new configuration using the **Add** option. Fill in the details.

5c Click **Start Reconfiguration**.

Manual Installation

With Change Guardian 5.0 and later, two communication profiles, legacy (`profile_iqc`) and the newer enhanced (`profile_javos`) are available. In case of the enhanced communication profile, download and use host specific certificates for each agent host along with agent artifacts to complete the manual installation.

For reference, the communication profile that Change Guardian uses is determined as indicated in the table below:

Table 3-1 *Change Guardian Profile Types*

Profile Type	Description
`profile_iqc` (legacy)	The Change Guardian server upgrade path includes version 4.2.1 or earlier, but the communication profile is not explicitly switched to `profile_javos`.
`profile_javos` (enhanced)	The Change Guardian server is a clean install of version 5.0 and later or the profile is explicitly switched to `profile_javos` in case of an upgrade to version 5.0 and later.

For more information, see Secure Communication Profile

Agent Certificates and Artifacts

You must use Change Guardian Agent Manager to download and install agent artifacts and certificates on one or more hosts.

NOTE: You can use agent artifacts and certificates only for the server specified and one at a time.

To download agent certificates and artifacts:

1 Log in to the Administration Console.

2 Click **Integration** > **Agent Manager**.

3 Click **All Assets** > **Manage Installation** > **Download**.

4 Select the **Agent certificates and artifacts** package.

5 Specify the hostname and the IP address, and then click **Start Download**.

6 Copy and extract `ChangeGuardianAgentCertificates.zip` file to the agent artifact directory, before installing the agents.

To manually install Change Guardian Agent for Windows:

1 From Administration Console click, **Integration** > **Agent Manager**.

2 Click **All Assets**, and then click **Manage Installation** and select **Download**.

3 Download the agent artifacts and certificates. See “Agent Certificates and Artifacts” on page 34 for the procedure.

4 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.

5 Copy `ChangeGuardianAgentforWindows.zip` to the computer where you want to install the Change Guardian Agent for Windows and extract the files.

Agent artifacts include: `NetIQCGAgentSilentInstaller.exe` and `NetIQCGAgentSilentInstaller.config`. The configuration file contains the configuration you chose when you downloaded agent artifacts.

NOTE: Both agent artifacts and certificates should be in the same directory to successfully complete the installation.

---

6 Change directory to the location where you extracted the files, right-click `NetIQCGAgentSilentInstaller.exe` file and select **Run as administrator** option.

Installing Security Agent for UNIX

For information about installing Security Agent for UNIX, see *Security Agent for UNIX documentation*.

Installing SmartConnector for Change Guardian

To collect events from Dell EMC and Microsoft Exchange assets, you must install the SmartConnector for Change Guardian to collect events in common event format (CEF).

At the time of installation, consider the following:

- SmartConnector for Change Guardian and the assets must be members of the same domain.
- You must not install the agent on a Domain Controller.

Pre-task for Microsoft Exchange PowerShell:

1 Open **Local Group Policy Editor.**

2 Go to **Local Computer Policy** > **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Windows PowerShell**.

3 Set **Turn on Script Execution** to Enabled.

4 Set **Execution Policy** to **Allow local scripts and remote signed scripts**.

To install SmartConnector for Change Guardian:

1 Download SmartConnector for Change Guardian from the Agent Manager.

2 Open the `SmartConnectorForChangeGuardian-7.14.exe` to launch the SmartConnector Installer for Change Guardian.

3 In the installer window, do the following:

- Specify the local path in which you want to install the SmartConnector for Change Guardian.
- Select the connector to configure:
  - **EMC Unity and VNXe Storage:** To monitor Dell EMC
  - **Microsoft Exchange PowerShell:** To monitor Microsoft Exchange
- Specify the location to store events in CEF.
- Values for **File Rotation Interval** and **File Size**.

  File Rotation Interval is the interval, in seconds, at which a new file is created. A new file is created when either the File Rotation Interval or the file size, in MB, exceeds the set value.
- For Microsoft Exchange PowerShell, enter the FQDN and the PowerShell path.

4 Open Windows services, and restart the required services:

- **ArcSight Dell EMC Unity and VNXe Storage**
- **ArcSight Microsoft Exchange PowerShell**

NOTE: Restart the services only once after the installation. Due to limitations on ArcSight SmartConnector, after the installation, the change events are not generated in CEF. Restarting the appropriate services start generating events in CEF.

Post Installation Configuration for Microsoft Exchange PowerShell

You must configure SmartConnector for Change Guardian services to run as the user who has access to receive exchange audit log.

To run the services as a domain administrator:

1 Open Windows services, and select **ArcSight Microsoft Exchange PowerShell**.

2 Open **Properties**, click **Log On**.

3 Click **This Account** > **Browse** > **Locations**, and select the domain name.

4 Specify the domain administrator credentials.

For information about uninstallation, and conceptual information about ArcSight SmartConnector, see the following guides at "*ArcSight Connectors Documentation*" site.

- MS Exchange PowerShell
- Dell EMC Unity and VNXe Storage
- SmartConnector User Guide

Configuring Change Guardian

After installing the Change Guardian server, you can configure the following.

If you want Change Guardian to run in FIPS mode, you must complete additional steps. For more information, see "Configuring FIPS 140-2" on page 37.

- "Configuring Memory Settings" on page 37
- "Configuring Server Date and Time Synchronization" on page 37

Configuring Memory Settings

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.

Configuring Server Date and Time Synchronization

To determine the current date and 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.

Verifying 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`*

Configuring FIPS 140-2

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.

To configure Change Guardian to run in FIPS mode:

1 As a root user, ensure that Mozilla Network Security Services (NSS) and Mozilla NSS Tools are installed on the Change Guardian server.

NOTE: For SLES 12 SP3, to enable FIPS mode, you must install `libfreebl3-hmac` and `libsoftokn3-hmac` packages.

---

2 (Conditional) If you want to change the keystore password, from a command prompt on the Change Guardian server, perform the following steps:

2a Switch to a `novell` user.

2b Change directory to `/opt/novell/sentinel/bin`.

2c Enter the `chg_keystore_pass.sh` script

Follow the on-screen prompts to change the `web server` keystore passwords. You will need this password later in this procedure.

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

```
./convert_to_fips.sh
```

4 Provide the requested input:

4a When asked whether to backup the server, select **n**.

4b Provide a password that meets the stated criteria. You will need this password later in this procedure.

4c (Conditional) Provide the password for the `Web Server` keystore (the password you created in Step 2 on page 38)

4d When asked whether to enter the external certificate in the keystore database, select **n**.

4e When asked whether to restart the Sentinel server, select **y**.

5 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
```

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

```
./convert_to_fips.sh
```

7 Provide the password for the FIPS keystore database (the password you created in Step 4b on page 38).

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

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

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

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

```
./convert_to_fips.sh
```

11 Provide the requested input:

11a Create the password for the FIPS keystore database.

11b Re-enter the password specified in Step 11a on page 39.

11c When asked whether to restart the Agent Manager service, select **y**.

12 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
```

Changing Default Email Host Settings

You can change the Default Email Host Settings in Change Guardian by use the following commands: `cd /opt/netiq/cg/scripts`

```
./configure.sh udei
```

NOTE: To configure secure connection with STARTTLS, set the following options: `--secure-connection=true`

Verifying the Installation

You can determine whether the installation is successful by performing one of the following:

- Ensure the server is running: `netstat -an | grep LISTEN | grep 8443`
- Ensure the appropriate server ports are open:
  - On SLES, run the following command on the server:

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

  - On RHEL, run the following command on the server:

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

  For more information about the ports used, see “Understanding Ports Used” on page 17.
- Access the Change Guardian dashboard:

  `https://IP_Address_Change_Guardian_server:8443/cg-main-ui/`

4 Getting Started

This chapter helps you start using newly installed Change Guardian.

Understanding the Change Guardian Interfaces

Change Guardian provides the following user interfaces:

For more information about the Change Guardian interfaces, see the *Change Guardian User Guide*.

Change Guardian Web Console

Following are the web-based interfaces:

Change Guardian Dashboard

The Change Guardian dashboard is the new dashboard that provides an quick view of events generated as a result of preconfigured policies. For more information, see Change Guardian Dashboard in the Change Guardian User Guide.

Administration Console

The Administration Console is the main user interface for viewing and interacting with Change Guardian data. As an administrator, you can perform tasks, such as:

- Create users.
- Configure LDAP settings.
- Search and view events.
- Creating event and alert routing rules.
- Create filters and tags for events.

Threat Response Dashboard

The Threat Response Dashboard is the main user interface for viewing and triaging alerts. For more information, see Threat Response Dashboard in the *Change Guardian User Guide*.

Agent Manager

Agent Manager provides a central location from where you can manage your agents directly on the agent machine or remotely install and update agents on assets. You can perform the following tasks using Agent Manager:

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

  NOTE: However, you can roll back the updates.

- Set configuration of the agents.
- Collect the installation logs.
- Start, stop and restart agents remotely.

Understanding Assets

An asset is a device that you can monitor using Change Guardian. In Agent Manager 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 see the last heartbeat time from the asset.

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.

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.

Agent Manager displays the following 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 categorize 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 organize 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.

Adding Assets

You have to add assets using Agent Manager to associate them with the Change Guardian agents.

To add assets in Agent Manager

1. Log in to Change Guardian, click **Integration** > **Agent Manager**.
2. (Conditional) If no assets were added in Agent Manager, then perform the following steps:
   - **2a** Click **All Assets**.
   - **2b** Click **Manage Assets** > **Add**.
3. (Conditional) If you have previously added assets in Agent Manager, then perform the following steps:
   - **3a** Under A**sset Groups**, click **All Assets**.
   - **3b** Click **Add Assets**.
4. (Conditional) To import assets from Active Directory, use the **Active Director** tab.

   NOTE: If you are using Active Directory over SSL or TLS connections, ensure that you have imported the Active Directory SSL certificate to the Change Guardian server. For more information, see “Configuring Certificates” on page 48.
5. (Conditional) To import assets from a text file, use the **Hosts List** tab.

   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 MajorType column, specify whether the operating system is UNIX or Windows.
6. (Conditional) To manually add an asset, use the **Host** tab.

Policy Editor

This is the interface that allows you to configure and manage policies. For information about policies, see Chapter 6, “Configuring Policies,” on page 91.

Policy Editor allows to perform tasks, such as:

- Manage application licenses.
- Assign policies to assets.
- Create and manage policy sets.
- Manage asset groups by adding assets to static and dynamic groups.
- Create administrative reports such as license utilization, manage assets, assigned policies by assets, and so on.
- Create alert rules.
- Configure event destinations.
- Schedule monitoring.
- Configure emails.

Viewing Assets in Policy Editor

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 see the last heartbeat time from the asset.

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.

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.

Adding a License Key

You must add licenses for both the Change Guardian server and the applications or modules that you plan to monitor. For more information about licenses, see "Understanding Licensing" on page 15.

If you are using the trial license key, you must add the enterprise license key before the temporary key expires to avoid any interruption in the Change Guardian functionality. For information about how to purchase the license, see the Change Guardian Product Web site.

- "Adding License for Server" on page 44
- "Adding License for Modules or Applications" on page 45

Adding License for Server

You can use the UI or the command-line to add a Change Guardian server license key.

- "Adding from the Administration Console" on page 44
- "Adding from the Command Line" on page 45

Adding from the Administration Console

To add a license key by using the Administration Console, follow the steps below.

To add a license key:

1. From Administration Console, click **About** > **Licenses**.
2. In the **Licenses** section, click **Add License**.

3 Specify the license key in the Key field. After you specify the license, the following information is displayed in the Preview section:

- Features: The features that are available with the license.
- Hostname: This field is for internal Novell use only.
- Serial: This field is for internal Novell use only.
- EPS: Event rate built into the license key. Beyond this rate, Change Guardian generates warnings but will continue to collect data.
- Expires: Expiry date of the license. You must specify a valid license key before the expiry date to prevent an interruption in functionality.

NOTE: If the license expired, you can add the license key by using only the command line.

---

4 Click **Save**.

Adding from the Command Line

To add a license key by using the command line, follow the steps below.

To add a license key:

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

2 Change to the `/opt/novell/Change Guardian/bin` directory.

3 Enter the following command to change to the novell user:

```
su novell
```

4 Specify the following command to run the `softwarekey.sh` script.

```
./softwarekey.sh
```

5 Enter 1 to insert the license key.

6 Specify the license key, then press Enter.

Adding License for Modules or Applications

Module Manager provides you information about licensed modules or applications, allows you to import application licenses to the Policy Editor, and allows you to remove application licenses from the Policy Editor.

When you install Change Guardian, all available applications are installed automatically. You must import the license key for each new application to start monitoring.

To import a license:

1 Log in to Policy Editor, click **Change Guardian**.

2 Select **Module Manager**

3 Click **Import License Key**.

4 Select the license key for the required application.

To add a new application to Module Manager:

1 In Module Manager, click **Install** > **From Local Directory**.

Configuring Security Settings

This section provides information about the configuring the following for secured communication.

Network Communication Options

Various components of Change Guardian communicate across the network and there are different types of communication protocols used throughout the system. All of these communication mechanisms affect the security of your system.

Secure Communication Profile

Change Guardian provides two security profiles for communication, `profile_iqc` and `profile_javos`:

- The legacy, `profile_iqc`, is the default on any Change Guardian installation prior to version 5.0. To avoid breaking of communication between components in your Change Guardian environment, you must continue to use `profile_iqc` provided one or more of the following statements are true:
  - One or more of your Change Guardian Agent for Windows instance versions is prior to 5.0.
  - One or more of your PE client instance versions is prior to version 5.0.
  - One or more of your Security Agent for UNIX instance versions is prior to 7.5.1.
  - One or more of your Security Agent for UNIX instances is being used for both Change Guardian and Secure Configuration Manager.
  - You want to continue using UNIX Agent Manager to install or upgrade your Security Agent for UNIX, instead of Change Guardian Agent Manager.
- The enhanced, newer, `profile_javos` is more secure and the default profile on any Change Guardian installation 5.0 and later. You can switch Change Guardian and all it’s components to use `profile_javos` if all of the following are true:
  - All Change Guardian components (Change Guardian Server, Policy Editor clients and Change Guardian Agent for Windows) are upgraded to version 5.0 and later.
  - All Security Agent for UNIX instances are upgraded to 7.5.1 and later.
  - You are ready to use Change Guardian Agent Manager for all future management of Security Agent for UNIX; UNIX Agent Manager is not compatible with the `profile_javos`.
  - Your instances of Security Agent for UNIX are not being used for both, Change Guardian and Secure Configuration Manager.

Configuring TLS

The Change Guardian server, agents, and Policy Editor components allow TLS 1.0 for communication. To improve the security posture and to prevent known vulnerabilities, you can disable TLS 1.0.

Following sections provide information about configuring TLS.

Prerequisites of Disabling TLS 1.0

You can disable TLS 1.0 manually after completing the following prerequisites:

- Upgrade Change Guardian Agent for Windows to 5.0 or later.
- Upgrade Security Agent for UNIX to 7.5.1 or later.
- Ensure that TLS 1.1 or a higher version is enabled for the SMTP server configured in Policy Editor.
- Ensure that you have Microsoft .NET Framework 4.5 or later on Policy Editor clients and all Windows and Active Directory machines you must monitor.

Disabling TLS 1.0

To disable TLS 1.0:

1. Log in as `novell` user.
2. Edit the `/opt/novell/sentinel/jdk/jre/lib/security/java.security` file.
3. Add TLSv1 to the list of disabled algorithms as follows:

   Before: `jdk.tls.disabledAlgorithms=SSLv3, RC4, MD5withRSA, DH keySize < 768`

   After: `jdk.tls.disabledAlgorithms=SSLv3, TLSv1, RC4, MD5withRSA, DH keySize < 768`

   When TLSv1 is included in the list of disabled algorithms, it forces the use of TLS 1.1 or above.
4. Run the following command to restart the Change Guardian server:

   ```
   /opt/netiq/cg/scripts/cg_services.sh restart
   ```

Enabling TLS 1.0

By default, TLS1.0 is disabled for new installations.

NOTE: You must not enable TLS1.0, unless you want to ensure compatibility between the agents which support TLS1.0 and the Change Guardian server. For example, Security Agent for UNIX prior to 7.5.1 or an SMTP server using only TLS 1.0.

Perform the following steps on the Change Guardian Server:

1. Log in as `novell` user.
2. Edit the `/opt/novell/sentinel/jdk/jre/lib/security/java.security` file.

3 Delete TLSv1 from the list of disabled algorithms as follows:

Before: `jdk.tls.disabledAlgorithms=SSLv3, TLSv1, RC4, MD5withRSA, DH keySize < 768`

After: `jdk.tls.disabledAlgorithms=SSLv3, RC4, MD5withRSA, DH keySize < 768`

4 Run the following command to restart the Change Guardian server:

```
/opt/netiq/cg/scripts/cg_services.sh restart
```

Configuring Certificates

To configure trusted connections when authenticating to the Administration Console, you must install valid certificates on the Change Guardian server.

Following sections provide information about configuring certificates.

- "Installing the Certificates" on page 48
- "Using CA-Signed Certificate" on page 49

Installing the Certificates

Use the command line tool provided on the Change Guardian server to install the certificates.

To install certificates on the server:

1 Switch user to `novell`.

2 Go to `/opt/novell/sentinel/setup` directory.

3 (Optional) 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 Get your generated `.csr` file signed by a certificate authority (CA)

4 Copy the 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 by using 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 signed by certificate authority**.

5e When prompted, select **Web Server**.

5f Specify the name of the file that contains the CA's signed digital certificate.

5g Select another service if necessary, or select **Done** and exit from the service option.

6 At the menu prompt, select **Exit** to exit from the TLS/SSL certificate configuration.

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

8 Import the CA root certificate change to the computer where you use the Administration Console.

Using CA-Signed Certificate

You can use CA-signed certificates in place of the self-signed certificates that is provided by Change Guardian.

To replace the self-signed certificates on the server:

1. Switch user to `novell`.
2. Create a backup of the existing `certs` folder, which is located at `/opt/netiq/cgutils/certs`.
3. Create a new `certs` folder at `/opt/netiq/cgutils/`.
4. Copy the CA-signed certificates to `/opt/netiq/cgutils/certs`
5. Change the permission of the `certs` folder by using the following command:

   ```
   chmod 700 /opt/netiq/cgutils/certs
   ```
6. Rename the CA-signed certificate files as below:
   - `cgca-cert.pem`: The root CA certificate
   - `cgca-pk.pem`: The private key
   - `cgca-pk.pem.pass`: The private key password
7. Change the ownership of the CA-signed files by running the following command: `chown novell:novell /opt/netiq/cgutils/certs/*`
8. Go to the `/opt/netiq/cgutils/bin` directory and run the following command:`./cg_cert_setup.sh`

   The required certificates are created in the `/opt/netiq/cgutils/certs/` directory.
9. To verify that the new certificates have the new CA name in the issuer field, run the following commands:
   - `openssl x509 -in amsca-cert.pem -noout -text`
   - `openssl x509 -in javosca-cert.pem -noout -text`
10. Go to `/opt/netiq/ams/ams/bin` directory and run the following commands:

    10a `./ams_cert_setup.sh --setup --profile=`*`ams_new_profile_name`*

    10b `./ams_cert_setup.sh --enable --profile=`*`ams_new_profile_name`*

    NOTE: It is recommended to keep the default profiles and create the profile with a different name.
11. To confirm that the profile is enabled, run the following command: `./ams_cert_setup.sh --show`
12. Go to `/opt/netiq/cg/javos/bin/` directory and run the following commands:

    12a `./javos_cert_setup.sh --setup --profile=`*`javos_new_profile_name`*

    12b `./javos_cert_setup.sh --enable --profile=`*`javos_new_profile_name`*
13. To confirm that the profile is enabled, run the following command: `./javos_cert_setup.sh --show`
14. (Conditional) If the Change Guardian server is in FIPS mode, then run the following commands:

    14a `./opt/netiq/ams/ams/bin/convert_to_fips.sh`

    14b `./opt/netiq/cg/javos/bin/convert_to_fips.sh`
15. (Optional) To test if the certificates are replaced successfully, remotely deploy an agent using Agent Manager and generate an event.

Applying Updates for Security Vulnerabilities in Embedded Third-Party Products

Change Guardian contains embedded third-party products such as JRE, Jetty, PostgreSQL, and ActiveMQ. Change Guardian includes patches to address the security vulnerabilities (CVE) for these products when updates for Change Guardian are released.

However, each of these products has its own release cycle, which means that there might be CVEs that are discovered before a Change Guardian update is released. You need to separately review the CVEs for each embedded third-party product, and decide whether to apply these updates to your Change Guardian system outside of the Change Guardian updates.

If you decide to apply patches to address these CVEs outside of a Change Guardian update, contact Technical Support.

Configuring LDAP

You can configure a Change Guardian server for LDAP authentication to enable users to log in to Change Guardian with their LDAP directory credentials. On the other hand, Change Guardian uses LDAP to process each user group in a policy as a list of the group members.

Following sections provide information about configuring LDAP.

- "Configuring LDAP for Authentication" on page 50
- "Configuring LDAP to Access Domain Controller" on page 53

Configuring LDAP for Authentication

LDAP authentication can be performed either using an SSL connection or an unencrypted connection to the LDAP server.

You can configure the Change Guardian server for LDAP authentication either with or without using anonymous searches on the LDAP directory.

- **Anonymous:** When you create Change Guardian LDAP user accounts, the directory user name must be specified and the user distinguished name (DN) does not need to be specified.

  When the LDAP user logs in to Change Guardian, the Change Guardian server performs an anonymous search on the LDAP directory based on the specified user name, finds the corresponding DN, then authenticates the user log in against the LDAP directory by using the DN.
- **Non Anonymous:** When you create Change Guardian LDAP user accounts, the user DN must be specified along with the user name.

  When the LDAP user logs in to Change Guardian, the Change Guardian server authenticates the user log in against the LDAP directory by using the specified user DN and does not perform any anonymous search on the LDAP directory.

NOTE: If anonymous search is disabled on the LDAP directory, you must not configure the Change Guardian server to use anonymous search.

- "Setting Up LDAP Authentication" on page 51
- "Logging in by Using LDAP User Credentials" on page 53

Setting Up LDAP Authentication

Perform the following procedure to set up LDAP authentication:

Prerequisite: Enable TLS 1.1 and TLS 1.2 protocols on your SSL enabled AD computer by adding appropriate registry keys for server and client.

1. From Administration Console, click **Users** in the toolbar.
2. On the **Users** page, click the **LDAP Settings** tab.
3. Specify the following to configure LDAP authentication:

   Host: Specify the hostname or the IP address of the LDAP server.

   This is a required field if you select the SSL option.

   SSL: Select this option if you want to connect to the LDAP server by using a Secure Socket Layer (SSL) connection.

   Port: Specify the port number for the LDAP connection. The default SSL port number is 636 and the default non-SSL port number is 389.

   Certificate File Path: Specify the path of the CA certificate file for the LDAP server.

   This field should be used only if you selected the SSL option and if the LDAP server certificate is not signed by well-known CA and is not trusted by default.

   Anonymous Search: Select **Yes** to perform anonymous searches or select **No** if you do not want to perform anonymous searches on the LDAP directory.

   Base DN: Specify the root container to search for users, such as o=netiq for eDirectory or CN=administrator,CN=users,DC=<example>,DC=<com> for Active Directory.

   - **If Anonymous Search is Yes:** Specify the root container in the LDAP directory to search for users.

     This is optional for eDirectory, and mandatory for Active Directory. For eDirectory, if the Base DN is not specified, the entire directory is searched to locate the users.
   - **If Anonymous Search is No:** Specify the root container in the LDAP directory that contains the users.

     This is mandatory if you are using Active Directory and if you set a domain name. For all other cases, this is optional.

   Search Attribute: Specify the LDAP attribute holding the user log in name. This is used to search for users.

   For example:

   - eDirectory:

     `uid`
   - Active Directory:

     `sAMAccountName`

   This field is available only if you selected **Yes** for Anonymous Search.

   Domain Name: Specify the name of the Active Directory domain.

   This is an additional approach applicable only for Active Directory for performing LDAP authentication without using anonymous search.

   When you specify the Domain Name, username@domainname (userPrincipalName) is used to authenticate the user before searching for the LDAP user object.

   For example, test.example.com

This field is applicable only for Active Directory and is available only if you selected **No** for Anonymous Search.

NOTE: If **Base DN** is set and **Domain Name** is not set, the **Base DN** is appended to the relative user DN to construct the absolute user DN.

For example, if the Base DN is set to `o=netiq` and the absolute user DN is `cn=sentinel_ldap_user,o=netiq` when the LDAP user account is created, only the relative user DN of `cn=sentinel_ldap_user` can be specified.

---

4 Click **Test Connection** to test whether the LDAP connection is successful.

4a Specify the test credentials to connect to the LDAP server:

If Anonymous Search is Yes: Specify the user name and password.

If you selected No for Anonymous Search and did not specify the Domain Name:

Specify the user DN and password. The user DN can be relative to the Base DN.

The **User DN** is based on the RFC 2253 standard. According to RFC 2253, when some reserved special characters are used as literals in a **User DN**, they must be escaped with a backslash (\). The following characters must be escaped:

- A space or # character occurring at the beginning of the string
- A space character occurring at the end of the string
- One of the characters , +, ", \, <, > or ;

For more information, see RFC 2253 (http://www.ietf.org/rfc/rfc2253.txt).

For example, if the **User DN** contains a comma (,) as a literal, specify the **User DN** as follows:

```
CN=Test\,User,CN=Users,DC=netiq,DC=com
```

eDirectory or Active Directory might require additional characters to be escaped. Refer the eDirectory or Active Directory documentation for any additional characters to be escaped.

If you selected No for Anonymous Search and specified the Domain Name: Specify the user name and password.

4b Click **Test Connection** to test the LDAP connection.

A message is displayed that indicates whether the connection is successful.

If there is an error, review the configuration details you provided and test the connection again.You can determine the cause of the failure by examining the `/var/opt/novell/sentinel/log/server0.0.log` file. You must ensure that the test connection is successful before saving the LDAP settings.

5 Click **Save** to save the LDAP settings.

On successful configuration:

- The `LdapLogin` section of the `/etc/opt/novell/sentinel/config/auth.login` file is updated. For example:

```
LdapLogin {
        com.sun.security.auth.module.LdapLoginModule required
java.naming.ldap.factory.socket="com.esecurity.common.communication.ProxyL
dapSSLSocketFactory"
        userProvider="ldap://10.0.0.1:636/o=netiq"
        userFilter="(&(uid={USERNAME})(objectclass=user))"
        useSSL=true;
};
```

- The LDAP server CA certificate, if provided, is added to a keystore named `/etc/opt/novell/sentinel/config/.ldapkeystore.jks`.

After saving the LDAP settings successfully, you can create LDAP user accounts to enable users to log in to Change Guardian by using their LDAP directory credentials.

NOTE: You can also configure the Change Guardian server for LDAP authentication by running the `ldap_auth_config.sh` script in the `/opt/novell/sentinel/setup` directory.

The script also supports command line options. To view the command line options, run the script as follows:

```
/opt/novell/sentinel/setup/ldap_auth_config.sh --help
```

Logging in by Using LDAP User Credentials

After you successfully configure the Change Guardian server for LDAP authentication, you can create Change Guardian LDAP user accounts. For more information on creating LDAP user accounts, see “Creating Users” on page 57.

After you create the LDAP user account, you can log in to the Change Guardian by using your LDAP user name and password.

Configuring LDAP to Access Domain Controller

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. You can also browse Active Directory to select items for use in a policy.

To access and configure the domain controller in LDAP settings:

1. In Policy Editor, click **Settings** > **LDAP Settings**.
2. In the LDAP Settings window, click **New**.
3. Specify the following fields:

   Domain name Specify the name of the Active Directory domain. For example, `test.example.com`

   User name Specify the name of the Active Directory user name. You can specify the user name in the following format:

   - `<user_name>`

- <domain_name\user_name>
- <user_name@domain_name.com>

Password Specify the password for the Active Directory user.

Polling interval It is the time interval at which the Change Guardian server synchronizes with the active directory for delta information.

4 Click **Test**, to test the authentication of the Active Directory user before searching for the LDAP object.

5 Click **Apply** to save the configuration.

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

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

Configuring Users and Roles

You can create different user roles and assign them different permissions. Role assignment helps you control users access to functionality, data access based on fields in the incoming events, or both. Each role can contain any number of users. Users belonging to the same role inherit the permissions of the role they belong to. You can set multiple permissions for a role.

Following sections provide information about configuring users and roles.

Overview

Change Guardian has the following roles by default:

Administrator: A user in this role has administrative rights in the Change Guardian system. You cannot delete users in this role. Administrative rights include the ability to perform user administration, data collection, data storage, search operations, rules, report, dashboard, and license management.

You cannot modify or delete the administrator role.

Change Guardian Administrator: A user in this role can view all event data, including raw data.

Event Dispatcher A user in this role can send only events and attachments to the server.

Operator A user in this role can manage alerts, view Security Intelligence Dashboards, share alert and event views, run reports, view and rename reports, and delete report results.

PCI Compliance Auditor: A user in this role has access to view events that are tagged with at least one of the regulation tags such as PCI, SOX, HIPAA, NERC, FISMA, GLBA, NISPOM, JSOX, and ISO/IEC_27002:2005, and can view system events, view the Change Guardian configuration data, and search data targets.

User: A user in this role can manage dashboards, run reports, view and rename reports, and delete report results.

Creating Roles

Roles allow you define what a user can manage and what data they can view. Permissions are granted to the role, and then the user is assigned to the role.

Creating a Role

1. From Administration Console, click **Users** in the toolbar.
2. Select a tenant from the **Tenants** list to assign a tenant to the role.

   Users created under this role will have access to view events from the selected tenant.
3. Click **Create** in the **Roles** section to create a new role.
4. Use the following information to create the role:

   Role name: Specify a unique name for the role. A role name should not exceed 40 characters.

   Description: Specify a description of the role.

   Users with this role can: Select the permissions that a role grants to users assigned to the role.

   - **View all event data:** Select this option to allow users to view all the data in the Change Guardian system. If you select this option, you must select one or more of the following permissions:
   - **View the following data:** Select this option to allow users to view only selected data in the Change Guardian system.
     - **Only events matching the criteria:** Allows users to view only the events returned by the specified search query. For example, if you set the filter value to `sev:5`, users with this permission can view only events of severity five in a search.
     - **Search Data Targets:** When this permission is set on a role, all members of that role can perform searches on Change Guardian systems that are in a distributed location.
     - **View asset data:** Allows users to view asset data.
     - **View asset vulnerability data:** Allows users to view vulnerability data.
     - **View data in the embedded database:** Allows users to view the data in the embedded database.
     - **View people browser:** Allows users to view the data in the Identity Browser.
     - **View system events:** Allows users to view the Change Guardian system events.
   - **Allow users to access reports:** Select this option to allow users to access and manage reports.
     - **Manage reports:** Allows users to create, modify, run, and delete reports.
     - **Run reports:** Allows users to only run reports.
   - **Allow users to manage alerts:** Select this option to allow users to view and manage alerts. Select either of the following options:
     - **Manage all alerts:** Allows the users to view and edit all the alerts and configure alert creation.
     - **Manage only alerts that match the following criteria:** Allows the users to view and edit the alerts that match the specified criteria. This permission also allows the role to configure alert creation.
   - **Sharing:** Allows users in the role to share real-time views, filters, and reports with other users.

- **Miscellaneous:** Assign miscellaneous permissions as necessary:
  - **Edit knowledge base:** Allows users to view and edit the knowledge base in the **Alert Details** page.
  - **Manage Tags:** When this permission is set on a role, all members of this role can create, delete, and modify tags, and associate tags to different event sources.
  - **Manage roles and users**: Allows non-administrator users to administer specific roles and users.
  - **Send Events and Attachments:** Allows users to send events and attachments to the server.

    NOTE: You must manually assign this permission to a user who needs to forward events to the server.
  - **Proxy for Authorized Data Requestors**: When this permission is set on a role, the members of this role can accept searches from remote data sources.
  - **View and execute event actions:** When this permission is set on a role, all members of this role can view events and execute actions on the selected events.
  - **View detailed internal system state data:** When this permission is set on a role, all members of this role can view detailed internal system state data by using a JMX client.
  - **View knowledge base:** Allows users to view the knowledge base in the **Alert Details** page.

5 Click **Save**.

To create users for this role, see “Creating Users” on page 57.

Understanding Password Complexity

A complex password improves security by preventing password guessing attacks. Change Guardian provides a set of password validation rules that help you maintain a complex password for all local user passwords. You can select the desired validation rules as applicable for your environment.

You can configure the password validation rules in the `/etc/opt/novell/sentinel/config/passwordrules.properties` file. The validation rules apply only to the local user passwords and not LDAP user passwords. For existing users, validation rules apply only after the users update their password.

By default, all the validation rules are disabled and commented with #. To enable validation rules, uncomment the rules, specify the values for the rules, and save the file.

The following table describes the password complexity validation rules:

Table 4-1 *Password Complexity Rules*

Validation Rule	Description
MINIMUM_PASSWORD_LENGTH	Specifies the minimum number of characters required in a password.
MAXIMUM_PASSWORD_LENGTH	Specifies the maximum number of characters allowed in a password.

Validation Rule	Description
UNIQUE_CHARACTER_LENGTH	Specifies the minimum number of unique characters required in a password. For example, if the UNIQUE_CHARACTER_LENGTH value is 6 and a user specifies the password as "aaaabbccc", the Change Guardian does not validate the password because it contains only 3 unique characters a, b, and c.
LOWER_CASE_CHARACTERS_COUNT	Specifies the minimum number of lowercase characters required in a password.
UPPER_CASE_CHARACTERS_COUNT	Specifies the minimum number of uppercase characters required in a password.
ALPHABET_CHARACTERS_COUNT	Specifies the minimum number of alphabetic characters required in a password.
NUMERIC_CHARACTERS_COUNT	Specifies the minimum number of numeric characters required in a password.
NON_ALPHA_NUMERIC_CHARACTERS_COUNT	Specifies the minimum number of non-alphanumeric or special characters required in a password. The rule considers only the following non-alphanumeric characters: ` ~ ! @ # $ % ^ & * ( ) - _ = + [{] } \ | ; : ' " < , > . / ?
RESTRICTED_WORDS_IN_PASSWORD	Specifies the words that are not allowed in a password. The restricted words are case-insensitive. You can specify multiple words separated by a comma. For example,RESTRICTED_WORDS_IN_PASSWORD= admin,password,test

Creating Users

Adding a user in the Change Guardian system creates an application user who can then log in to Change Guardian. You also assign roles when you create the user.

1. From Administration Console, click **Users.**
2. Click **Create** in the **Users** section.
3. Specify the name and email address of the user.

   The fields with an asterisk (*) are mandatory, and the user name must be unique.

   A user name cannot exceed 30 characters, and you can use extended characters when you create it.
4. Select a role for the user.
5. Select the authentication type:

   Local: Select this option for the server to authenticate the user log in against the internal database. By default, the **Local** option is selected.

   Directory: The **Directory** option is enabled only if you have configured the Change Guardian server for LDAP authentication. Select this option for the server to authenticate the user log in against an LDAP directory.
6. (Conditional) If you specified Local for the authentication type in Step 5, specify any user name in the **Username** field and continue with Step 8.

7 (Conditional) If you specified Directory for the authentication type in Step 5, specify the user name according to the settings you used when you configured LDAP, then continue with Step 10.

8 Specify a password in the **Password** field.

NOTE: For local user password, ensure that the password adheres to the password complexity validation rules. For more information, see “Understanding Password Complexity” on page 56.

---

9 Re-enter the password in the **Verify** field.

10 The **Title**, **Office #**, **Ext, Mobile #**, **and Fax.** fields are optional. The phone number fields allow any format. Make sure you enter a valid phone number so that the user can be contacted directly.

11 Click **Save**.

5 Configuring Event Monitoring

Change Guardian provides monitoring of change events of your assets. An asset could be a system running on Windows, Linux, UNIX, Group Policy, Windows Active Directory, Microsoft Azure Active Directory, Microsoft Exchange, NetApp, and Dell EMC.

This section provides information about configuring the following assets.

Configuring Windows Active Directory Monitoring

Change Guardian monitors the following Windows Active Directory (AD) sources:

- AD objects
- Computer accounts
- Configurations
- Contacts
- Groups
- User accounts
- Organization units
- Trusts

You must configure your Active Directory environment to ensure that the operating system generates and retains Active Directory events until Change Guardian processes them. This chapter provides information about the following:

For information about requirements and recommendations for computers running the Active Directory Domain Services, see the Technical Information for Change Guardian 5.2 page.

Implementation Checklist

The following table provides an overview of the tasks required for Change Guardian to start monitoring Windows Active Directory audit events:

Task	See
Complete the prerequisites	“Prerequisites” on page 60
Add the license key	“Adding a License Key” on page 44
Configure the Windows Active Directory	“Configuring the Security Event Log” on page 60
	“Configuring Active Directory Auditing” on page 61
	“Configuring User and Group Auditing” on page 62
	“Configuring Active Directory Security Access Control Lists” on page 63
	“Synchronizing Active Directory User Accounts” on page 128
Configure Change Guardian for monitoring	“Creating Windows Active Directory Policies” on page 66
	“Assigning Policies and Policy Sets” on page 95
Triage events	Chapter 7, “Managing Events,” on page 99
	Chapter 8, “Configuring Alerts,” on page 105

Prerequisites

Ensure that you have completed the following:

- Install Change Guardian Agent for Windows
- Install Policy Editor

Configuring Active Directory

You have to complete the following tasks to configure Active Directory

- “Configuring the Security Event Log” on page 60
- “Configuring Active Directory Auditing” on page 61
- “Configuring User and Group Auditing” on page 62
- “Configuring Active Directory Security Access Control Lists” on page 63

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**.

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 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, select the following options:

- Configure the following audit events
- Success
- Failure

6d For CGAD only, define the same configuration for all subcategories of **Account Management** and **Policy Change**.

7 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 Select the following options:

- **Define these policy settings**
- **Success**
- **Failure**

7d 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**.

Configuring User and Group Auditing

This configuration enables auditing of user logon and logoff activities (by both local users and Active Directory users), and local user and group settings.

You can configure user and group auditing by one of the following methods:

- "Configuring Manually" on page 62

Configuring Manually

You can configure user and group auditing manually.

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 Select **Default Domain Controllers Policy**, and then click **OK**.

7. Click **Finish**, and then click **OK**.
8. In the Microsoft Management Console, expand **Default Domain Controllers Policy *FQDN* > Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Audit Policy**.
9. Under **Audit Account Logon Events**, select **Define these policy settings**, and then select **Success** and **Failure**.
10. Under **Audit Logon Events**, select **Define these policy settings**, and then select **Success** and **Failure**.
11. 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**.
12. Under **Audit Logon**, select **Audit Logon**, and then select **Success** and **Failure**.
13. Under **Audit Logoff**, select **Audit Logoff**, and then select **Success** and **Failure**.
14. To update Group Policy settings, open a command prompt and type `gpupdate /force`.

Configuring Active Directory Security Access Control Lists

The 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 "Configuring SACLs for Change Guardian for Active Directory" on page 63. If you are running Change Guardian for only Group Policy in your environment, see "Configuring SACLs for Change Guardian for Group Policy Only" on page 65.

Configuring SACLs for Change Guardian for Active Directory

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

To verify or set this configuration:

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. In the **Applies to** or **Apply onto** field, select **This object and all descendant objects**.
11. Configure auditing to monitor every user.
    - If you are using Windows Server 2012 or later:
        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 **Permission** 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 versions lower than Windows 2012:
        1. Type `everyone` in the **Enter the object name to select** field.
        2. Click **OK**.
        3. In the **Permission**, 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.
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.

Configuring SACLs for Change Guardian for Group Policy Only

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

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 **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. Clear the setting to **Apply these auditing entries to objects and/or containers within this container only**.
11. Configure auditing to monitor every user.
    - If you are using Windows Server 2012 or later:
        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 **Permission** list, select the following:
            - **Delete**
            - **Create Organizational Unit objects**
        6. In the **Properties** list, select the following:
            - **Write gPLink**
            - **Write gPOptions**
    - For versions lower than Windows 2012:
        1. Type `everyone` in the **Enter the object name to select** field.
        2. Click **OK**.
        3. In the **Permission** list, select the following:
            - **Delete**
            - **Create Organizational Unit objects**
        4. In the **Properties** list, select the following:
            - **Write gPLink**
            - **Write gPOptions**
12. Click **OK** until you close all open windows.

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

Creating Windows Active Directory Policies

You can create policies to monitor the following event sources:

AD objects Polices for creating and deleting domain, modifying connection object, and so on.

Computer accounts Polices for disabling and moving computer account, and changing permission to accounts.

Configurations Policies for creating and deleting GPOs.

Contacts Policies for creating, deleting, moving, and changing permission to contact.

Groups Policies for modifying DNS configurations, and monitoring node and zone.

User accounts Policies for creating distribution group, changing membership, creating security group, and so on.

Organization units Policies for creating, deleting, moving, and changing permission on organization unit.

Schema Policy templates and view policy templates.

Trusts Policies for creating, deleting, and modifying trust.

For more information about creating policies, see “Creating Change Guardian Policies” on page 92.

After creating policies, you can assign them to assets. For information about assigning policies, see “Working with Policies” on page 94.

NOTE: When you assign the Active Directory schema policies which are created for Attribute and Class schema monitoring together to the monitor assets, the AD schema events are not generated successfully.

Configuring Microsoft Azure Active Directory Monitoring

Azure Active Directory (Azure AD) is Microsoft’s cloud based directory and identity management service. Change Guardian allows you to monitor Azure AD along with on-premises Active Directory. You can use the Azure AD feature to improve employee productivity, streamline IT processes, improve security, and cut costs.

The Azure AD monitoring capability in Change Guardian is built in conjunction with Microsoft Graph API. You must understand the technical limitations of the reporting APIs that are captured in Azure Active Directory reporting latencies documentation.

Change Guardian supports real-time monitoring, but due to Microsoft Azure’s latency limitations, there is a delay in fetching audit logs. This can be overcome when Microsoft fixes this latency issue.

IMPORTANT: Change Guardian supports monitoring on the Microsoft Azure public cloud. For more information, see Microsoft Graph REST API v1.0 reference.

Change Guardian monitors the following in Azure AD:

- Administrative units
- Applications
- Devices
- Directories
- Groups
- Policies
- Resources
- Roles for users and groups
- User accounts

For more information about Azure AD, see Azure AD documentation.

Figure 5-1 *Communication Between Change Guardian Components in an Azure AD environment*

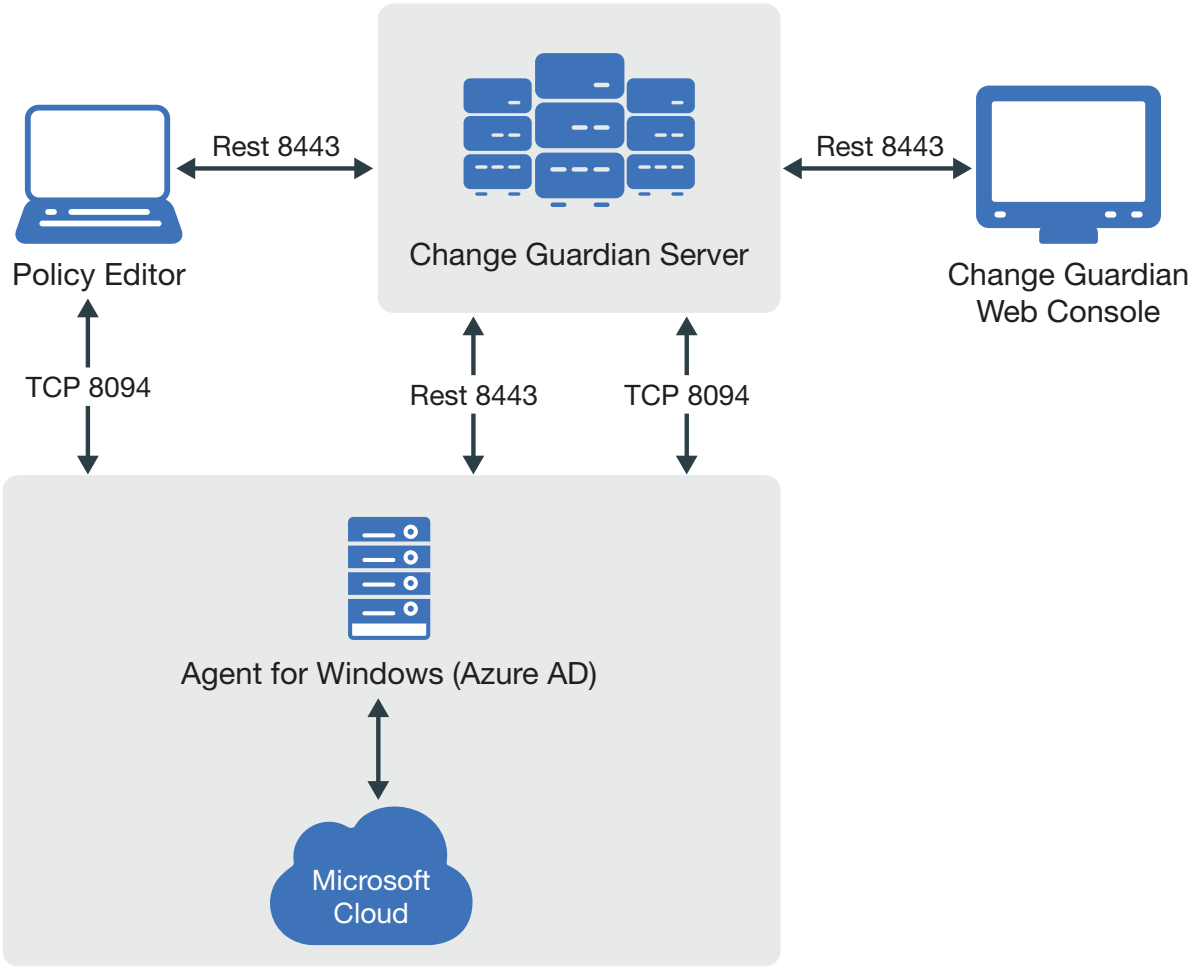
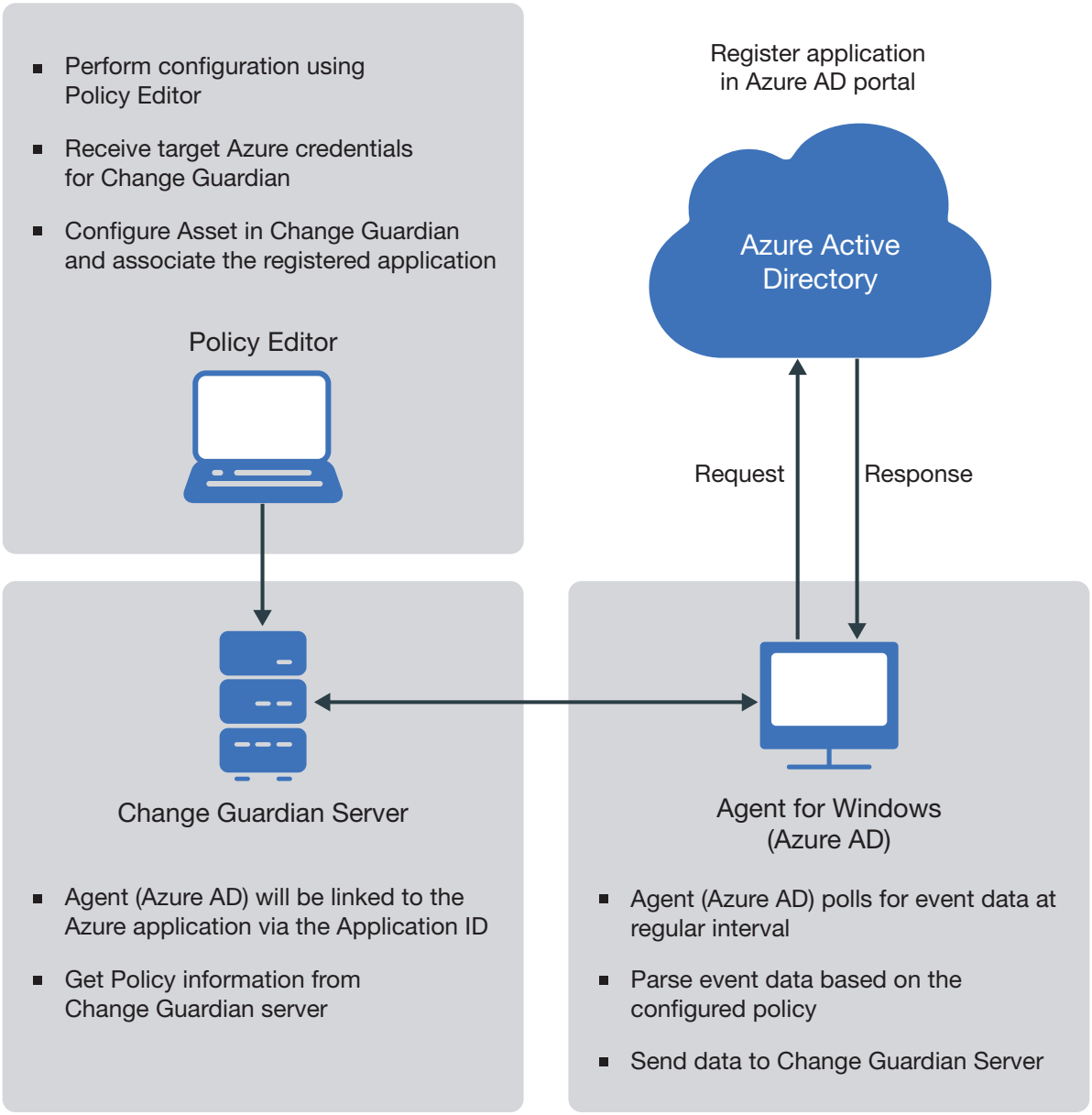


Figure 5-2 *Actions Performed by the Change Guardian Components in an Azure AD environment*



Implementation Checklist

The following table provides an overview of the tasks required for Change Guardian to start monitoring Azure AD audit events:

Task	See
Complete the prerequisites	“Prerequisites” on page 70

Task	See
Ensure that you have created a tenant and its credentials are available for Change Guardian. Required credential details: ◆ Domain Name ◆ Authentication Key ◆ Application ID	Microsoft Azure AD portal
Add the license key	“Adding a License Key” on page 44
(Conditional) Configure the default Windows registry keys, if you want to modify the default keys based on your requirements.	“Configuring Default Windows Registry Keys” on page 70
Configure Change Guardian for monitoring	“Enabling Azure AD Monitoring” on page 72 “Configuring Azure AD Tenant” on page 72 “Creating Azure AD Policies” on page 73 “Assigning Policies and Policy Sets” on page 95
(Conditional) During upgrade, ensure that you reconfigure the Change Guardian Agent for Windows to enable Azure AD monitoring.	“To reconfigure an agent using Agent Manager:” on page 33
Triage events	Chapter 7, “Managing Events,” on page 99 Chapter 8, “Configuring Alerts,” on page 105

The following illustration explains the work flow of various components namely: the server, agents, clients, Policy Editor and Microsoft Azure Active Directory.

Prerequisites

Ensure that you have completed the following:

- Install Change Guardian Agent for Windows
- Install Policy Editor

Configuring Default Windows Registry Keys

By default, Change Guardian has defined the default values for the Windows registry keys. If you want to modify the registry key values, perform the following procedures:

- “Configuring Azure AD Event Fetching Interval” on page 70
- “Configuring Azure AD Access Token Refresh Time Interval” on page 71
- “Configuring Azure AD Event Collection Interval” on page 71

Configuring Azure AD Event Fetching Interval

Change Guardian fetches events in given time intervals. The default interval, is set to the recommended 120 minutes, behind the *current system time* as the *start time*.

NOTE: If the time interval is set to more than 1440 minutes, the system resets it to 1440 minutes automatically, since that is the maximum value permissible. If the latency from Microsoft is more than this value, you might face data loss.

This recommendation is due to latency issues from the Microsoft Graph API. Also while processing events received from Azure AD, Change Guardian removes duplicate events if any internally. For more information, see Azure Active Directory reporting latencies.

If you observe a different latency time in your environment, you can change this value to the observed value.

To modify the time interval:

1. In Windows registry settings, navigate to the Change Guardian agent installation directory: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\NetIQ\ChangeGuardianAgent`
2. Right click the `AzureADEventFetchInterval` key.
3. Select **Decimal** under **Base**.
4. (Conditional) If you notice a higher latency value in your environment, you can configure this value based on your observed value. The value range is between 120 minutes to 1440 minutes (24 hours) for the **Value data** field.
5. Click **OK**.
6. Go to **Services** > **NetIQ Change Guardian Agent**.
7. Select theChange Guardian Agent for Windows application, then click **Restart**.

Configuring Azure AD Access Token Refresh Time Interval

By default, every 30 minutes, Change Guardian refreshes the access token used to connect to the Azure active directory. The maximum limit is 50 minutes. If you configure this value to below 15 minutes, the system will reset it to 15 minutes automatically. If you configure this value to above 50 minutes, the system will reset it to 50 minutes automatically.

To modify this time interval based on your requirement:

1. In Windows registry settings, navigate to the Change Guardian Agent installation directory: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\NetIQ\ChangeGuardianAgent`
2. Right click the `AzureADTokenRefreshInterval` key.
3. Select **Decimal** under **Base**.
4. Specify the time interval to any required value range between 15 minutes to 50 minutes in the **Value data** field.
5. Click **OK**.
6. Go to **Services** > **NetIQ Change Guardian Agent**.
7. Select the Change Guardian Agent for Windows application, then click **Restart**.

Configuring Azure AD Event Collection Interval

By default, Change Guardian fetches event logs every 10 minutes from the Azure Active Directory and processes them based on applied policies.

NOTE: The recommended duration for a fetch interval is 10 minutes.

You can configure a event collection interval to be any duration between 5 and 30 minutes. If you configure the duration to be below 5 minutes, the system resets it to 5 minutes automatically. Similarly if you configure the duration to be above 30 minutes, the system again resets it to 30 minutes automatically.

To modify this time interval based on your requirement:

1. In Windows registry settings, navigate to the Change Guardian Agent installation directory: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\NetIQ\ChangeGuardianAgent`
2. Right click the `AzureADEventCollectionInterval` key.
3. Select **Decimal** under **Base**.
4. Specify the time interval to any required value range between 5 minutes to 30 minutes in the **Value data** field.
5. Click **OK**.
6. Go to **Services** > **NetIQ Change Guardian Agent**.
7. Select the Change Guardian Agent for Windows application, then click **Restart**.

Configuring Change Guardian

Complete the following tasks on Change Guardian server to monitor Azure AD events:

- “Enabling Azure AD Monitoring” on page 72
- “Configuring Azure AD Tenant” on page 72
- “Creating Azure AD Policies” on page 73

Enabling Azure AD Monitoring

Reconfigure the Change Guardian Agent for Windows, using Agent Manager, to enable Azure AD monitoring.

Prerequisite: Ensure that you have added Azure AD assets in Agent Manager.

To reconfigure the agent

1. In Agent Manager, select the asset and click **Manage Installations** > **Reconfigure Agents**.
2. In the Reconfigure Agents page, edit the configuration to select **Enable Azure AD Monitoring**.

Configuring Azure AD Tenant

In Azure Active Directory (Azure AD), a tenant is a representative of an organization. You have to configure a tenant and its credentials such as Domain Name, Authentication Key, and Application ID and make it available to Change Guardian. Change Guardian connects with Azure Active Directory using the Microsoft Graph API. It supports a single tenant

---

NOTE: The Azure AD agent is supported on Windows platforms.

To configure the Azure AD tenant for monitoring using the Policy Editor:

1. In Policy Editor, select **Azure Active Directory** from the left panel.
2. From the tree, navigate to **Azure Tenant Configuration**.

3 In the **Azure Tenant Configuration** window, specify values for the following fields:
   - **Domain Name**: Specify the name of the Azure Active Directory domain.
   - **Application ID**: Enter the Application ID that was displayed in the Azure portal during configuration.
   - **Authentication Key**: Enter the Authentication Key that was displayed in the Azure portal during configuration.
   - **Comment**: (Optional) Enter a comment.
4 Click **Save**.
5 (Conditional) If you want to modify any particular configuration, you need to make the modifications in the **Azure Tenant Configuration** window.

Creating Azure AD Policies

You can create policies to monitor the following Azure AD event sources:

Administrative Unit : Policies for adding, deleting or updating administrative units, and modifying administrative unit attributes.

Applications : Policies for adding, deleting and updating applications and application owners.

Devices : Policies for adding, deleting and updating devices, and modifying device attributes.

Directories : Policies for adding verified and unverified domains, and modifying directory attributes.

Groups : Policies for adding, deleting, updating and restoring groups, adding and removing group owner and group member, and so on.

Policy : Policies for adding, deleting and updating policies, and modifying policy attributes.

User Accounts : Policies for adding, deleting, restoring and updating user accounts, disabling and enabling accounts, and changing user license and user password, and so on.

The following section provides information about how to create policies for Azure AD.

- “Creating a Policy for Azure AD Groups” on page 73
- “Creating a Policy For Azure AD User Accounts” on page 74

For more information about creating fresh policies, see “Creating Change Guardian Policies” on page 92.

After creating policies, you can assign them to assets. For information about assigning policies, see “Working with Policies” on page 94.

NOTE: You cannot assign Azure AD policies by using Asset Groups.

Creating a Policy for Azure AD Groups

Complete the following steps to create the Azure Active Directory policy using the Policy Editor

To add a policy:

1 In the left pane of the Policy Editor window, select **Azure Active Directory** > **Azure Active directory Policies**.
2 Expand the **Azure Active directory Policies** and select **Groups**.
3 On the **Groups Policy** window, specify the appropriate information.

NOTE: Specifying the specific group event type from the event list is mandatory.

4 Click **Submit**.

Creating a Policy For Azure AD User Accounts

Complete the following steps to create the Azure Active Directory policy using Policy Editor

To add a policy:

1 In the left pane of the Policy Editor window, select **Azure Active Directory** > **Azure Active directory Policies**.

2 Expand the **Azure Active directory Policies** and select **User Accounts**.

3 Click **Create Policy.**

4 On the **User Account Policy** window, specify the appropriate information.

NOTE: Specifying the specific user event type from the event list is mandatory.

5 Click **Submit**.

Troubleshooting

This section contains some of the issues that might occur when you want to monitor Azure AD, using Change Guardian, along with workarounds.

Change Guardian receives an Insufficient Access Permission event

Issue: Change Guardian is unable to receive events because *Read directory data* permissions are not assigned to the Azure AD web application for both Application and Delegated permission types.

Workaround: Assign *Read directory data* permission for both Application and Delegated Permission types to Azure AD web application for Change Guardian to receive events.

Change Guardian receives an Invalid Configuration event

Issue: Change Guardian is unable to receive events because of the incorrect Domain Name, Authentication Key, or Application ID used to access Azure AD.

Workaround: Use the correct Domain Name, Authentication Key, or Application ID to access Azure AD.

NOTE: Severity of Insufficient Access Permission and Invalid Configuration events vary based on the severity of the first policy assigned.

Change Guardian Is Unable to Receive Azure AD Events

Issue: Change Guardian is unable to receive events because of the following:

- Tenant is not reachable
- Invalid remote web application

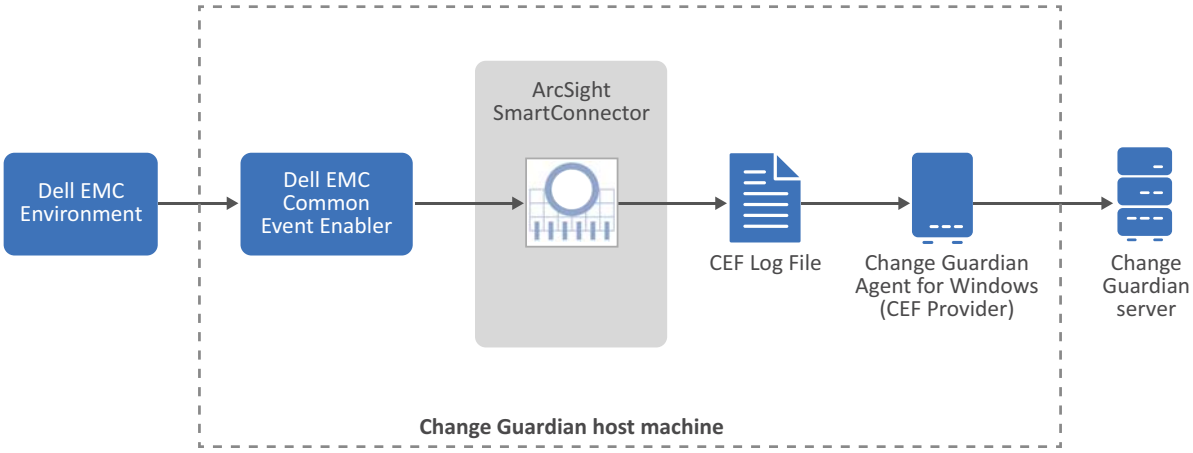
Workaround:

- Enter a valid tenant name in the tenant configuration page.
- Check if the tenant is accessible from the Change Guardian Agent computer.

Configuring Dell EMC Monitoring

Change Guardian monitors the Dell EMC file systems on Isilon and Unity storage platforms. This section provides information about the following.

Figure 5-3 *Dell EMC Monitoring using Change Guardian*



The deployment diagram illustrates the following:

- Dell EMC CEE collects events from the Dell EMC machine. For more information about Dell EMC CEE, see *"Using the Common Event Enabler for Windows"* in the Dell EMC website.
- SmartConnector for Change Guardian acts as the interface between Dell EMC and Change Guardian. It pulls event data from Dell EMC CEE and stores the event details in a CEF log file.
- Change Guardian Agent for Windows reads from the CEF log file and sends the event details to the Change Guardian server.

Implementation Checklist

Complete the following tasks to monitor Dell EMC:

Task	See
Complete the prerequisites	“Prerequisites” on page 76
Add a license key	“Adding a License Key” on page 44
Configure Change Guardian for Dell EMC monitoring	“Configuring Change Guardian” on page 76
	“Working with Policies” on page 94
Triage events	Chapter 7, “Managing Events,” on page 99
	Chapter 8, “Configuring Alerts,” on page 105

Prerequisites

Ensure that you have completed the following:

- Install SmartConnector for Change Guardian

  Install SmartConnector for Change Guardian and Dell EMC Common Event Enabler (CEE) on the same machine.
- Install Change Guardian Agent for Windows

  Install Change Guardian Agent for Windows on the same machine where you installed SmartConnector for Change Guardian.
- Install Policy Editor
- Install and configure CEE

Configuring Change Guardian

Complete the following procedures to configure Change Guardian to monitor Dell EMC events:

- “Enabling Dell EMC Monitoring” on page 76
- “Creating Dell EMC Policies” on page 77

Enabling Dell EMC Monitoring

You must configure Change Guardian server and SmartConnector for Change Guardian to receive Dell EMC event logs.

Prerequisites Ensure that you have added Dell EMC asset in Agent Manager.

To enable monitoring:

1. In Agent Manager, select the asset and click **Manage Installations** > **Reconfigure Agents**.
2. In the Reconfigure Agents page, edit the configuration to select **Enable Smart Connector Plugin**.
3. Specify the location to store CEF events in **CEF Data Output Path**.

NOTE: Ensure that the value in **CEF Data Output Path** matches the CEF data path that you had specified during SmartConnector for Change Guardian installation. You can get the CEF data path from `ceffolder` parameter in the `<install_directory>\current\user\agent\agent.properties`.

Creating Dell EMC Policies

You can create file system policies to generate events about files and directories when they are created, deleted, renamed, permission changed, and so on.

While creating file system policies, specify the EMC shared path in the following format: `\\hostname\device type identifier\local sub folder.`

For example for Isilon specify `\\onefs8104-1\onefs$\ifs\<local sub directory>`, and for Unity specify `\\onefs8104-1\CHECK$\ifs\<local sub directory>`. Here `\\onefs8104-1` is the host name and `\ifs\<local sub directory>` is the directory you want to monitor.

NOTE: It is recommended to monitor the file system of Dell EMC Unity storage. For example, specify the path as `\\Unity-1\CHECK$\LocalFS` in Policy Editor, where `LocalFS` is the Dell EMC Unity file system name.

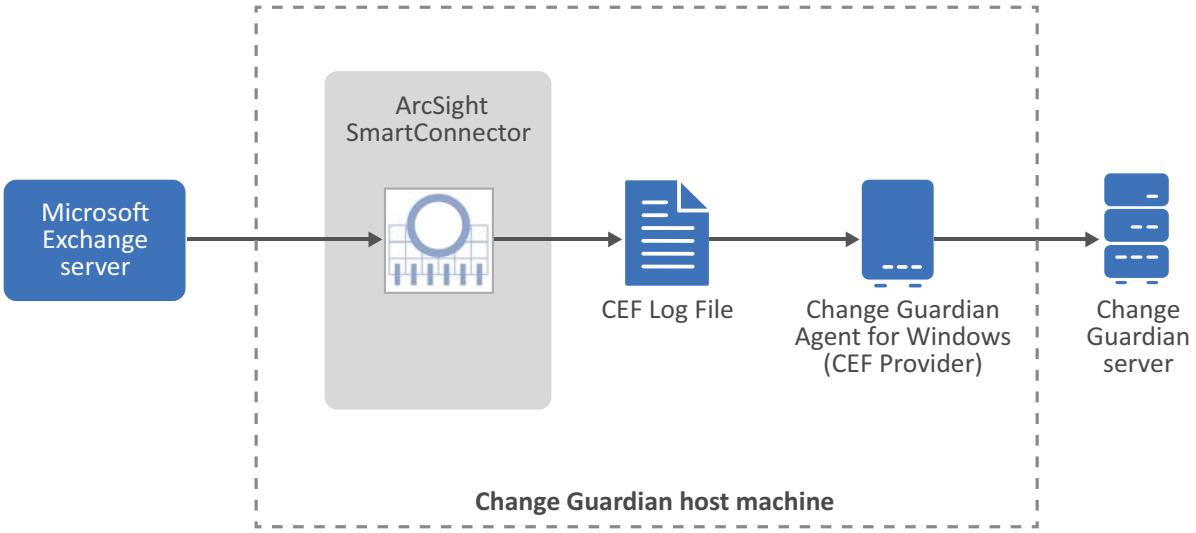
For information about creating policies, see “Creating Change Guardian Policies” on page 92.

After creating policies, you can assign them to assets. For information about assigning policies, see “Working with Policies” on page 94.

Configuring Microsoft Exchange Monitoring

Change Guardian monitors Microsoft Exchange settings, mailbox accounts, mailbox messages, management role groups, and rights.

Figure 5-4 *Microsoft Exchange Monitoring using Change Guardian*



The deployment diagram illustrates the following:

- SmartConnector for Change Guardian acts as the interface between Microsoft Exchange and Change Guardian. It pulls event data from Exchange and stores the event details in a CEF log file.
- Change Guardian Agent for Windows reads from the CEF log file and sends the event details to the Change Guardian server.

Implementation Checklist

The following table provides an overview of the tasks required for Change Guardian to start monitoring Microsoft Exchange events:

Task	See
Complete the prerequisites	“Prerequisites” on page 78
Add the license key	“Adding a License Key” on page 44
Configure Change Guardian for monitoring	“Enabling Exchange Monitoring” on page 79
	“Creating Microsoft Exchange Policies” on page 79
Triage events	You can triage events in the Change Guardian dashboard and the Administration Console.

Prerequisites

Ensure that you have completed the following in the same order:

IMPORTANT: Install SmartConnector for Change Guardian, Change Guardian Agent for Windows, and on the same machine as Microsoft Exchange.

1. Enable auditing in Microsoft Exchange
   - Enable Mailbox Auditing
   - Enable Administrator Auditing
   - Execute PowerShell Scripts
2. Install SmartConnector for Change Guardian
3. Install Change Guardian Agent for Windows
4. Install Policy Editor.

Configuring Change Guardian

You must complete the following tasks on Change Guardian server.

- “Enabling Exchange Monitoring” on page 79
- “Creating Microsoft Exchange Policies” on page 79

Enabling Exchange Monitoring

You must configure the Change Guardian server to receive the Exchange event logs from SmartConnector for Change Guardian.

Prerequisite: Ensure that you have added Exchange asset in Agent Manager.

To enable monitoring:

1. In Agent Manager, select the asset and click **Manage Installations** > **Reconfigure Agents**.
2. In the Reconfigure Agents page, edit the configuration to select **Enable Smart Connector Plugin**.
3. Specify the location to store CEF events **CEF Data Output Path**.

NOTE: Ensure that the value in **CEF Data Output Path** matches the CEF data path that you had specified during SmartConnector for Change Guardian installation. You can get the CEF data path from `ceffolder` parameter in the `<install_directory>\current\user\agent\agent.properties`.

Creating Microsoft Exchange Policies

You can create policies to the following event sources:

Exchange Settings : Policies for creating, deleting configuration settings.

Mailbox Accounts : Policies for creating, deleting and moving of mailbox accounts, and enabling and disabling mailbox accounts.

Mailbox Messages : Policies for sending, moving, deleting messages, and so on.

Management Role Groups : Policies for adding, deleting, and modifying role group, adding and removing group member, and so on.

For information about creating policies, see “Creating Change Guardian Policies” on page 92.

After creating policies, you can assign them to assets. For information about assigning policies, see “Working with Policies” on page 94.

NOTE: While creating mailbox policies, you do not have to configure LDAP settings to browse the Exchange server mailboxes.

Configuring Group Policy Monitoring

Change Guardian monitors the following:

- Group policies objects
- Preferences
- Settings
- Starter group policy objects
- SYSVOL

This section provides the following information:

Implementation Checklist

The following table provides an overview of the tasks required for Change Guardian to start monitoring Group Policy events:

Task	See
Complete the prerequisites	“Prerequisites” on page 80
Add the license key	“Adding a License Key” on page 44
Configure Change Guardian for monitoring	“Creating GPO Policies” on page 80
Triage events	You can triage events in the Change Guardian dashboard and the Administration Console.

Prerequisites

Ensure that you have completed the following:

- Install Change Guardian Agent for Windows.
- Install Policy Editor.

Creating GPO Policies

You can create policies to monitor the following event sources:

Group Policy Objects Policies for deleting and modifying group policies and domain policy.

Group Policy Preferences Policies for changes to local user and group preferences to GPO.

Group Policy Settings Policies for modifying software settings.

Starter Group Policy Objects Policies for creating, deleting, and modifying starter group policies.

SYSVOL Policies for changing Central Store and SYSVOL folder

For information about creating fresh policies, see “Creating Change Guardian Policies” on page 92.

After creating policies, you can assign them to assets. For information about assigning policies, see “Working with Policies” on page 94.

Configuring NetApp Storage Monitoring

Storage solutions like NetApp store a large amount of data and therefore can have a large volume of audit events. Change Guardian monitor changes to files and on the NetApp storage.

Change Guardian supports both CIFS (Common Internet File System) and NFS (Network File System) protocols for monitoring NetApp storage. You must use Security Agent for Unix 7.6 or later and also enable native auditing on the NetApp shares you want to monitor.

You can monitor and receive alerts for a variety of malicious behaviors that occur on a Network Attached Storage (NAS) device. For example, unauthorized user accessing confidential files and directories. You can also include or exclude certain files or from the audit scope to ensure a faster and more efficient audit process.

Implementation Checklist

Complete the following tasks to monitor NetApp shares:

Task	See
Complete the prerequisites	“Prerequisites” on page 81
Add a license key	“Adding a License Key” on page 44
Configure NetApp native auditing	“Configuring NetApp Native Auditing for CIFS” on page 82
	“Configuring NetApp Native Auditing for NFS” on page 83
Configure Change Guardian for NetApp monitoring	“Mounting the Audit Logs in CIFS” on page 84
	“Mounting the Audit Logs in NFS” on page 85
	“Creating a Configuration File” on page 85
Triage events	You can triage events in the Change Guardian dashboard and the Administration Console.

Prerequisites

Ensure that you have completed the following:

- Install the supported platforms and hardware. For more information, see Technical Information for Change Guardian 5.2.
- The NetApp share is in Data ONTAP 9. 1 Cluster Mode.
- Install Security Agent for UNIX.

NOTE: You should install Security Agent for UNIX on a dedicated system. This ensures that reading files from the agent system does not create file read events.

- Install Policy Editor.

Configuring the NetApp Native Auditing

You must configure the NetApp native auditing solution to monitor file and directory events on your SVM with a FlexVol volume.

The security descriptor may contain Discretionary Access Control Lists (DACLs) for applying to file and folder access permissions or SACLs for file and folder auditing, or even both SACLs and DACLs.

For better performance, store the audit file on a separate volume.

NOTE: If you use the `cat` command to create and modify a file in quick succession, you might find a missing `file modify` event as NetApp reads and updates audit logs slower than Linux.

You can configure NetApp auditing by using one of the following ways:

- "Configuring NetApp Native Auditing for CIFS" on page 82
- "Configuring NetApp Native Auditing for NFS" on page 83

Configuring NetApp Native Auditing for CIFS

You must create an auditing configuration on the given storage virtual machine (SVM) for CIFS, before you can monitor events on Windows systems. You can monitor these events over CIFS by setting SACLs (System Access Control List) on storage objects in NTFS or mixed mode volumes.

To configure auditing for CIFS:

1. Launch the Data ONTAP command-line interface.
2. Create audit configuration for an SVM by running the following command:

   ```
   vserver audit create -vserver <Name_SVM> -destination "/<Name_Volume>" -events file-ops -format xml -rotate-size XB -rotate-limit 10
   ```

   Example: When vserver name is `SVM1`, volume is `vol1` and folder `audit`, then the command should be :

   ```
   vserver audit create -vserver SVM1 -destination /vol1/audit -events file-ops -format xml -rotate-size 1MB -rotate-limit 10
   ```

3. Verify audit configuration by running the following command: `vserver audit show -vserver <Name_SVM>`

   For example, to verify audit configuration for SVM1, run the follwing command: `vserver audit show -vserver SVM1`

```
Vserver: SVM1
Auditing State: true
Log Destination Path: /vol1
Categories of Events to Audit: file-ops, cifs-logon-logoff,audit-policy-change
Log Format: xml
Log File Size Limit: 100MB
Log Rotation Schedule: Month: -
Log Rotation Schedule: Day of Week: -
Log Rotation Schedule: Day: -
Log Rotation Schedule: Hour: -
Log Rotation Schedule: Minute: -
Rotation Schedules: -
Log Files Rotation Limit: 0
```

4 Enable SVM auditing by running the following command: `vserver audit enable -vserver <Name_SVM>`

Example:

```
vserver audit enable -vserver SVM1
```

Configuring NetApp Native Auditing for NFS

You must create an auditing configuration on the given storage virtual machine (SVM) for NFS on an SVM to monitor events on Linux systems. Similarly, you can monitor these events over NFS by setting NFS 4.x ACLs (Access Control Lists) on UNIX or mixed mode volumes.

To configure auditing in NFS:

1 Launch the Data ONTAP command-line interface.

2 Create audit configuration for an SVM by running the following command:

```
vserver audit create -vserver <Name_SVM> -destination "/<Name_Volume>" -events
file-ops -format xml -rotate-size XB -rotate-limit 10
```

Example: When vserver name is `SVM1`, volume is `vol1` and folder `audit`, then the command should be :

```
vserver audit create -vserver SVM1 -destination /vol1/audit -events file-ops -
format xml -rotate-size 1MB -rotate-limit 10
```

3 Verify audit configuration by running the following command: `vserver audit show -vserver <Name_SVM>`

For example, to verify audit configuration for SVM1, run the following command: `vserver audit show –vserver SVM1`

```
Vserver: SVM1
Auditing State: true
Log Destination Path: /vol1
Categories of Events to Audit: file-ops, audit-policy-change
Log Format: xml
Log File Size Limit: 100MB
Log Rotation Schedule: Month: -
Log Rotation Schedule: Day of Week: -
Log Rotation Schedule: Day: -
Log Rotation Schedule: Hour: -
Log Rotation Schedule: Minute: -
Rotation Schedules: -
Log Files Rotation Limit: 0
```

4 Enable SVM auditing by running the following command: `vserver audit enable -vserver <Name_SVM>`

   Example:

   `vserver audit enable -vserver SVM1`

5 To configure Security Agent for UNIX to monitor the NetApp FileSystem changes, enable ACL for NFS by running the following command: `vserver nfs modify -vserver <name_SVM> -v4.0 enabled -v4.0-acl enabled`

   Example:

   `vserver nfs modify -vserver SVM1 -v4.0 enabled -v4.0-acl enabled`

6 Verify `nfs4-acl-tools` is installed on the NFSv4 Linux host:

   6a Run the `mkdir <Folder_Name>` command to create a mount directory.

   6b Mount to the directory by running the following command: `mount -t nfs4 <nas_SVMIP>:/<volume_name> <mount_path>`

   Example:

   If SVM IP is `x.x.x.x`, volume name is `vol1` and mount path is `/mnt/folder1`, run the following command: `mount -t nfs4 x.x.x.x:/vol1 /mnt/folder1`

   6c To monitor each folder within a volume, add audit flags recursively on each of the in the mount directory that you need to monitor: `nfs4_setfacl -R -a U:fdSF:EVERYONE@:rwaDdTNCo <NFS_Share>`

   Example:

   If a folder name in the volume is `NFSShare`, run the following command: `nfs4_setfacl -R -a U:fdSF:EVERYONE@:rwaDdTNCo NFSShare`

   6d To monitor an entire volume, add audit flags recursively on the mount directory which contains the volume mounted: `nfs4_setfacl -R -a U:fdSF:EVERYONE@:rwaDdTNCo <mount directory>`

   Example:

   If the mount directory is `/mnt/folder1`, run the following command: `nfs4_setfacl -R -a U:fdSF:EVERYONE@:rwaDdTNCo /mnt/folder1`

Configuring Change Guardian for NetApp Monitoring

Complete the NetApp audit configuration and mount the NetApp volumes into the Security Agent for Unix; one volume for audit logs and the other for CIFS or NFS shares to monitor.

Perform the following to configure the Change Guardian server:

- “Mounting the Audit Logs in CIFS” on page 84
- “Mounting the Audit Logs in NFS” on page 85
- “Creating a Configuration File” on page 85
- “Creating NetApp Policies” on page 86

Mounting the Audit Logs in CIFS

Create a mount point in the Security Agent for Unix computer, enter the NetApp configuration details in `/etc/fstab` and mount the audit log and the NetApp volume that contains the CIFS share.

1 Create a mount directory.

Example:

```
mkdir /mnt/audit
```

2. Go to `/usr/netiq/vsau/etc` and create new file named `cifs`.
3. Update the `cifs` file as follows:

   ```
   username=<user name>
   password=<password>
   domain=<domain name>
   ```

4. Change the permissions of this file to secure credentials in it using the following command:

   ```
   chmod 600 cifs
   ```

5. Update the `/etc/fstab` in the following format:

   ```
   <svm_ip>:/<volume> <mountlocation> cifs ro,nouser,noexec,nosuid,credentials=/
   usr/netiq/vsau/etc/cifs 0 0
   ```

   Example:

   ```
   10.0.0.1:/vol1 /mnt/audit cifs ro,nouser,noexec,nosuid,credentials=/usr/netiq/
   vsau/etc/cifs 0 0
   ```

6. Mount the audit volume to the mount location: `mount /mnt/audit`

NOTE: You must have read permissions to read the audit file.

Mounting the Audit Logs in NFS

Create a mount point in the Security Agent for UNIX computer, enter the NetApp configuration details in `/etc/fstab` and mount the audit log and the NetApp volume over NFS.

1. Create a mount directory: `mkdir /mnt/audit`
2. Update the `/etc/fstab` in the following format:

   ```
   <svm_ip>:/<volume> <mountlocation> nfs ro,nouser,noexec,nosuid 0 0
   ```

   Example:

   ```
   10.0.0.1:/vol1 /mnt/audit nfs ro,nouser,noexec,nosuid 0 0
   ```

3. Mount the audit volume to the mount location: `mkdir /mnt/audit`

NOTE: You must make changes to `/etc/fstab` and mount the volume with the NetApp share following the sequence of steps above.

Creating a Configuration File

Complete the following steps in Security Agent for UNIX:

1. Go to `/usr/netiq/vsau/etc` and create new file named `netapp-volume-tab`.
2. Update the `netapp-volume-tab` file in the following format: `SVM_IP_address, share, mount_directory, volume`

   Example:

   If SVM IP is `x.x.x.x`, share name is `vol1`, mount directory is `/mnt/audit`, volume name is `vol1`, then specify the command as follows:`x.x.x.x,/vol1,/mnt/audit,vol1`

NOTE: When you monitor an entire volume, you must update the NetApp volume tab as `x.x.x.x,/vol1,/mnt/audit,vol1`

Creating NetApp Policies

Create policies to monitor creating, deleting, renaming, and changing permission on NetApp files and directories.

NOTE: Specify the `/folder_name` that you want to monitor in the *directory* field of the policy definition. If you want to monitor at the SVM level, then just use */*instead of the folder name.

For information, see “Creating Change Guardian Policies” on page 92.

After creating policies, you can assign them to assets. For information about assigning policies, see “Working with Policies” on page 94.

Configuring Linux or UNIX Monitoring

In Linux and UNIX environment, Change Guardian monitors the following:

- Configuration files
- Local and exported file systems
- File integrity
- Users and groups
- Mounts
- Processes
- CRON jobs

This section provides the following information:

Implementation Checklist

The following table provides an overview of the tasks required for Change Guardian to start monitoring Linux and UNIX events:

Task	See
Complete the prerequisites	“Prerequisites” on page 70
Add a license key	“Adding a License Key” on page 44
Configure Change Guardian for monitoring	“Creating UNIX Policies” on page 87
	“Assigning Policies and Policy Sets” on page 95
Triage events	You can triage events in the Change Guardian dashboard and the Administration Console.

Prerequisites

Ensure that you have completed the following:

- Install the Security Agent for UNIX. For more information, Security Agent for UNIX documentation.
- Install Policy Editor.

Creating UNIX Policies

You can create polices to monitor the following:

Configuration Files Policies for changing hostname resolution and process startup configuration.

CRON Policies for monitor accessing CRON job, and changing CROS task execution.

Exported File System Policies to monitor list exported file system

File Integrity Policies to monitor Security Agent for UNIX configuration and system message of the day.

File System Policies to monitor bash shell startup configuration.

Groups Policies to monitor inbuilt groups

Mount Policies to monitor CD-ROM mounts

Process/Daemons Policies to monitor system background processes, and execution of `su` and `sudo` commands.

Users Policies to monitor builtin users.

For information about creating policies, see “Creating Change Guardian Policies” on page 92.

After creating policies, you can assign them to assets. For information about assigning policies, see “Working with Policies” on page 94.

Configuring Windows Monitoring

On a Windows environment, Change Guardian monitors the following:

- File integrity
- File shares
- File systems
- Local users and groups
- Processes
- Registry
- Removable media

NOTE: Change Guardian supports monitoring removable media events only on USB flash drives. To monitor external hard disk drive (HDD), create a file system monitoring policy on the mounted drive.

Implementation Checklist

The following table provides an overview of the tasks required for Change Guardian to start monitoring Windows events:

Task	See
Complete the prerequisites	“Prerequisites” on page 70
Add a license key	“Adding a License Key” on page 44
Configure Change Guardian for monitoring	“Creating Windows Policies” on page 88
	“Assigning Policies and Policy Sets” on page 95
Triage events.	You can triage events in the Change Guardian dashboard and the Administration Console.

NOTE: Change Guardian supports monitoring removable media events only on USB flash drives and Windows platform. To monitor external hard disk drive (HDD), create a file system monitoring policy on the mounted drive.

Prerequisites

Ensure that you have completed the following:

- Install Change Guardian Agent for Windows
- Install Policy Editor

Creating Windows Policies

You can create policies to monitor changes to the following:

- File integrity
- File shares
- File systems
- Local users and groups
- Processes
- Registry
- Removable media

NOTE: To enable the Registry Browser in Change Guardian, you must set the `repositoryEnabled` flag (under `HKLM\Software\Wow6432Node\NetIQ\ChangeGuardianAgent\repositoryEnabled`) to 1, and then restart the agent.

If you do not manually set the flag to 1, when you use the Registry Browser, you will receive a Could not connect to Windows Data Source error.

For information about creating policies, see “Creating Change Guardian Policies” on page 92.

After creating policies, you can assign them to assets. For information about assigning policies, see “Working with Policies” on page 94.

6 Configuring 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.

Understanding Policies

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.

Policy sets You can combine multiple policies from one or more modules, to be able 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.

NOTE: Event Severity is always calculated automatically for Security Agent for UNIX events, including events generated by policies configured with a custom severity.

Understanding Policy Attributes

Policy attributes provide granular details of a policy, such as the purpose, severity, and authorized users.

Event Severity When you create or edit a policy, you can specify a constant event 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. The following are examples:

- **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

Managed User 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 “Configuring LDAP” on page 50.

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.

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. You can also browse Active Directory to select items for use in a policy.

Creating Change Guardian Policies

You can create a policy in the one of the following methods:

- Create a fresh policy with no preconfigured settings
- Clone and customize an out-of-the-box template

Creating a Fresh Policy

You can create a fresh policy without preconfigured settings.

To create a policy:

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

- Windows
- Azure Active Directory
- NetApp share
- Dell EMC
- Microsoft Exchange

NOTE: Only the installed application are displayed.

2 Expand the list of policies and select the policy type you want to create, such as **Active 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 or privileges, or both that you want to monitor.

6 Click **Submit**.

7 (Conditional) If you want to enable the policy now, select the **Enable this policy revision now** check box

NOTE: For more information about enabling a policy, see “Enabling a Change Guardian Policy Revision” on page 96 .

Creating from a Template

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 from a template:

1 In the left pane of **Policy Editor**, select one of the following:

- Active Directory
- Group Policy
- UNIX
- Windows
- Azure Active Directory
- NetApp share
- Dell EMC
- Microsoft Exchange

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** check box

---

NOTE: For more information about enabling a policy, see “Enabling a Change Guardian Policy Revision” on page 96

Working with Policies

After creating a policy, you can perform various activities such as clone a policy, assign the policy, schedule policy monitoring:

Following sections provide more information about working with policies.

Cloning a Change Guardian Policy

Cloning an existing policy allows you to quickly create a policy based on an 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.

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 clones 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 from a template:

1 In the left pane of Policy Editor, select one of the following:

- Active Directory
- Group Policy
- UNIX
- Windows
- Azure Active Directory
- NetApp share
- Dell EMC
- Microsoft Exchange

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** check box

NOTE: For more information about enabling a policy, see "Enabling a Change Guardian Policy Revision" on page 96

Creating Change Guardian Policy Sets

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 **Change Guardian**.

2 Select **Policy Set Manager**.

After you create a policy set, you can assign the set as you would assign a policy. To assign policies, see "Assigning Policies and Policy Sets" on page 95

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.

You can use Policy Editor 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.

To assign a policy to an agent:

1 In the left pane of the Policy Editor window, navigate to **Change Guardian**.

2 Click **Policy Assignment**.

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

4 Select **Assets** from the drop-down list.

NOTE: You cannot assign Azure AD policies via **Asset Groups**.

5 Select a policy set or policy and click **Apply**.

NOTE: An existing policy or policy set that has already been assigned can only be edited from the way it was assigned. For example, if you want to add an event destination to a policy that was assigned via a Policy Set you must edit it in the policy set only. This also applies to the server and group assignment.

Enabling a Change Guardian Policy Revision

Change Guardian saves the policy in the Policy Repository on the Change Guardian server 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 work that is in progress. Use the Policy Editor to view all policy revisions as well as the version number of the currently enabled policy. You can also load a previous revision of a policy to edit or enable.

You must submit policies to the Policy Repository before you can enable or assign policies, or make policies available to others. Before you can assign a policy revision to monitor computers or asset groups, you must enable it. You can enable a policy revision as follows:

- When you submit the policy to the Policy Repository, after creating or editing it.
- From the history tab of the selected module window in case of an existing policy.

NOTE: After you enable a policy revision, you must assign the policy to computers or assets groups. If you update the enabled revision of a policy already assigned, Change Guardian automatically updates any monitored assets that have that policy with the new revision but only when the agent requests at the next heartbeat.

To enable a policy revision from an application or 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**.

Exporting and Importing Change Guardian 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 also modify an imported policy to create a new policy with a similar definition. However, you can export one policy at a time but import multiple policies at a time.

To export a policy:

1. In the left pane of the **Policy Editor** window, navigate to the policy that you want to export.
2. Right-click the policy, and select **Export**.

To import a policy:

1. From the Policy Editor menu window, click **Settings** > **Import Policies**.
2. Select the required `.xml` file, and click **Open**.

Assigning Event Destinations to Change Guardian 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**.

Scheduling Change Guardian Policy Monitoring

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**.

Administrative Reports

Change Guardian allows you to create administrative 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.

Use the Policy Editor console to access administrative reports. Select the needed report type run the report. to generate it. The available report options are as follows:

- License Utilization.
- Assigned Policies by Asset.
- Asset Monitoring Failures.
- Assets by Assigned Policies.

- Managed Assets.
- Policies not Assigned.

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

7 Managing Events

This chapter provides information about managing events by setting the event destination other than the Change Guardian server, setting event routing rules based on set filters, create event tags, storing events for long-term retention.

Configuring 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.

A policy must have at least one event destination. When you create a policy, it automatically uses the default event destination which is the Change Guardian server. You can also assign the policy to the syslog server or a third party security information and event management (SIEM) tool.

You can create and assign additional event destinations to meet your environment and regulatory needs. You can also change the default event destination. If you set another event destination as the default, all new policies automatically use the new default location. Existing policies continue to use their previously assigned event destinations. To change the event destinations for existing policies, see “Assigning Event Destinations” on page 101.

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 “Configuring Event Destinations to Generate Alerts” on page 108.

You can configure Change Guardian agents to send events to Sentinel, to leverage Sentinel capabilities. Starting with Sentinel 8.2, you can use the HTTP Server Connector and distribute Change Guardian assets across multiple Sentinel Collector Managers and multiple Event Source Servers to scale data collection. For information about the HTTP Server Connector, see the Connector documentation on the Sentinel Plug-ins Website. For information about Sentinel, see Sentinel Documentation.

Following sections provide information about creating event destinations.

Creating Event Destinations

Change Guardian evaluates the event routing rules on a first-match basis in top-down order and applies the first matched event routing rule to events that match the filter criteria. You can configure event routing rules to evaluate and filter all incoming events and deliver selected events to designated output actions. For example, each severity 5 event can be logged to a file.

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

- **REST Dispatcher** - Forwards Change Guardian events directly from a Change Guardian agent to the Change Guardian or Sentinel server.

  NOTE: If you add an event destination, ensure that the user account associated with that destination has permissions to send events and attachments.

- **Syslog Dispatcher** - Forwards Change Guardian events from Change Guardian agent to Change Guardian server, which in turn forwards events to third-party SIEM or syslog server.

  NOTE: Change Guardian supports the Common Event Format (CEF) specification and could use Syslog Dispatcher to forward events. Related event attributes might contain additional backslash (\) characters to escape the following characters: \, =, and | and allow the event to conform to CEF. To remove them, parse the events with a CEF parser.

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 of the server where you want to send events.

   For Sentinel, if you have deployed remote Collector Managers to receive events from Change Guardian assets, specify the IP address of the Collector Manager and port number of the Event Source Server. Otherwise, specify the IP address and port number of the Sentinel server.

   NOTE: While changing the event destination, ensure that the new destination server is running on FIPS mode, if the Change Guardian server runs on FIPS mode.

7. (Optional) If you want to send Change Guardian system events that only match specific criteria, select the check box above the filter drop-down list, and provide filter criteria.

   NOTE: The filter is applied to all event destinations configured on the server.

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

NOTE: If more than one event destinations are configured on a Change Guardian server, specifying one event destination while creating a policy ignores the specified destination and sends events to all the configured event destination.

For Sentinel, if you have deployed Collector Managers to receive events from Change Guardian assets, you must create an event destination for each Event Source Server.

Assigning Event Destinations

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 takes 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 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**.

Configuring Event Routing Rules

You can configure event routing rules to filter events based on one or more of the searchable fields. You can associate each event routing rule with one or more of the configured actions. You can also assign tags to group the events logically.

Following sections provide information about configuring event routing rules.

- "Creating Event Routing Rules" on page 101
- "Ordering Event Routing Rules" on page 102
- "Activating or Deactivating an Event Routing Rule" on page 103

Creating Event Routing Rules

You can create a filter-based event routing rule and then assign one or more configured actions that are executed to handle or output the events that meet the event routing rule criteria.

To create an event routing rule:

1. From Administration Console, click **Routing** in the toolbar.
2. Click **Create**, then use the following information to create a new event routing rule:

   Name: Specify a unique name for the event routing rule.

   Criteria: Select a saved criteria to use in creating event routing rule. This criteria determines which events are stored in the event store.

   Select tag: (Optional) Select a tag for tagging the filter. The tag makes the filter more specific.

   Route to the following services: Select where the information is routed. The options are:

   - **All:** Routes the event to all services including Correlation, Security Intelligence, and Anomaly Detection.
   - **Event store only:** Routes the event to the event store only.

- **None (drop):** Drops or ignores the events.

Perform the following actions: Select an action to be performed on every event that meets the filter criteria. The following default actions are available for event routing rules:

- Log to File
- Log to Syslog
- Send Events via Sentinel Link
- Send SNMP Trap

NOTE: When you associate an action with routing rules, ensure that you write rules that match a small percentage of events, if the rule triggers a Javascript action. If the rules trigger actions frequently, the system might backlog the actions framework. This can slow down the EPS and might affect the performance of the Change Guardian server.

For the actions to work, you must have configured the Integrator associated with each action for your environment.

Select the email configuration that you already created using Policy Editor. For more information see Chapter 9, “Configuring Email Notifications,” on page 111.

The actions listed here are different than the actions displayed in the **Event Actions** tab in the Administration Console, and are distinguished by the `<EventRouting>` attribute in the `package.xml` file created by the developer.

Adding or Removing Actions You can add more than one action to perform on the events that meet the filter criteria:

3 Click **Save** to save the event routing rule.

The newly created event routing rule appears at the end of the rules list under the **Event Routing Rules** tab. By default, this new event routing rule is active.

Ordering Event Routing Rules

When there is more than one event routing rule, the event routing rules can be reordered by dragging them to a new l ocation. Events are evaluated by event routing rules in the specified order until a match is made, so you should order the event routing rules accordingly. More narrowly defined event routing rules and more important event routing rules should be placed at the beginning of the list.

The first routing rule that matches the event based on the filter is processed. For example, if an event passes the filter for two routing rules, only the first rule is applied. The default routing rule cannot be reordered. It always appears at the end.

To order event routing rules:

1 From Administration Console, click **Routing** in the toolbar.

The **Event Routing Rules** tab is displayed.

Existing event routing rules appear on the page.

2 Mouse over the icon to the left of the event routing rule numbering to enable drag-and-drop. The cursor changes.

3 Drag the event routing rule to the correct place in the ordered list.

When the event routing rules are ordered, a success message is displayed.

Activating or Deactivating an Event Routing Rule

New event routing rules are activated by default. If you deactivate an event routing rule, incoming events are no longer evaluated according to that event routing rule. If there are already events in the queue for one or more actions, it might take some time to clear the queue after the event routing rule is deactivated. If the **On** check box next to the event routing rule is selected, the event routing rule is activated. If the **On** check box is not selected, the event routing rule is deactivated.

1. From Administration Console, click **Routing** in the toolbar.

   The **Event Routing Rules** tab is displayed.

   Existing event routing rules appear on the page.
2. To activate the event routing rule, select the check box next to each event routing rule in the **Enabled** column.

   If the event routing rule is activated, a success message is displayed.
3. To deactivate the event routing rule, select the check box next to each event routing rule in the **Enabled** column.

   When the event routing rule is deactivated, a success message is displayed.

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 Sentinel. For more information, see “Configuring Data Storage” in the *Sentinel Administration Guide*.

Viewing Events

To view events, see the “Viewing Events” in the *Change Guardian User Guide*.

8 Configuring 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. Alerts notify you of what is most important for you to look at. Alerts can relate to threats to IT resources or performance thresholds such as system memory full or IT resources not responding.

This chapter provides the following information:

Understanding Alerts

Change Guardian automatically associates the relevant events and identities with the alert to help you determine the root cause of 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.

Managing Alerts

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.

During the regular life cycle of an alert, a user does the following:

- Opens an alert view and either pick an alert already assigned to them or claim an unassigned alert.
- Views 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.
- Determines the next step and add comments about the decision:
  - Close as harmless
  - Respond appropriately, and then close
  - Investigate further

Creating and Managing Alert Rules

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 Administration 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.

- "Creating Alert Rules" on page 106
- "Redeploying Alert Rules" on page 107
- "Configuring Event Destinations to Generate Alerts" on page 108

Creating 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.

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.

NOTE: If you are using Change Guardian in a mixed environment with 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.

Policy Editor allows you to create, delete, edit, redeploy, and view alerts.

To create an alert rule:

1. Log in to Policy Editor.
2. To open Alert Rules window, click **Settings** > **Alert Rules**.
3. Select an alert view:
   - All alert rules
   - Alert rules grouped according to the associated event destination
4. Specify the following details:
   - The alert rule name of your choice.

     The alert rule name supports only alphanumeric characters and underscores. Special characters, such as `-!`~#$%^&()+=[],;.` and space, are not supported
   - The policy or policies that you want to be alerted on.

If you do not specify one or more policies, the alert rule is applicable for all policies.

- The option to create an alert with a filter for a specific pattern.

  For example to select every policy name with DNS in the title, the alert rule creates alerts for all policies that contain `DNS` in the policy name, such as `DNS Configuration`.
- Whether you want to be alerted on severity and severity range.
- The event name or event names that you want to be alerted on.

  You can optionally add additional granularity by adding event name as filter criteria when you create any alert rule.

  Following are a few categories for event names:

  - Active Directory
  - Configuration
  - File Systems
  - Group
  - Group Policy
  - Processes
  - User Accounts
  - Windows Specifics
- The event field or event fields that you want to be alerted on.
- Whether you want to be alerted on managed or unmanaged users.
- Whether you want to be alerted on event outcome.
- Whether you want to be alerted on IP address and its subnet.
- 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 attributes.
- The event destinations to which you want to deploy the alert rule. By default, all available event destinations are selected.

NOTE: When you create an alert rule, Change Guardian uses the user account logged into Policy Editor. You can also associate a different user account with an additional event destination. Both of these user accounts must have `Manage all alerts` and `Manage Correlation Engines/Rules` permissions.

Redeploying Alert Rules

When you create an alert rule and save, 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 and save, the alert rule is also redeployed automatically, to the given event destination. You can also redeploy the alert rule manually. 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 the “Viewing and Triaging Alerts in Alert Views” in the *Change Guardian User Guide*.

Configuring Event Destinations to Generate 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.

To ensure all event destinations receive alerts:

1. Download the certificates from the following location, and place them in a temporary location, such as `/tmp`:

   `file: /etc/opt/novell/sentinel/config/sentinel.cer`
2. Change the credentials as follows:
   - `# chown novell:novell /path to certificate`
   - `# chmod 644 /path to certificate`
3. At the 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.

Creating and Managing Alerts Routing Rules

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.

- "Creating an Alert Routing Rule" on page 108
- "Ordering Alert Routing Rules" on page 109

Creating an Alert Routing Rule

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.

To create an alert routing rule to filter the alerts:

1. Log in to the Administration 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.

Analyzing Alerts

To analyze alerts, see the "Viewing Alerts" in the *Change Guardian User Guide*.

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 Administration 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.

9 Configuring Email Notifications

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

- Use the Policy Editor to:
  - Add each email server to Change Guardian.
  - Create one or more notification groups for each email server.
- Use the Administration Console to assign email alerts to specified events. For more information, see “Creating Rules to Send Emails” on page 113.

This chapter provides the following information.

Configuring Email Servers

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.

Configure Email Servers to Change Guardian in FIPS Mode

To configure email servers to Change Guardian running in FIPS mode, perform the following steps.

To add email server to Change Guardian:

1. Export the certificate from the respective SMTP server site.
2. Browse to the Sentinel bin directory. The default location is `/opt/novell/sentinel/bin`.
3. Import the certificate using the following command: `convert_to_fips -i <certificate_path>`.
4. Restart the Change Guardian server using the following command: `rcsentinel restart`.
5. Add new email configuration with STARTTLS protocol using Policy Editor.
6. Create routing rules in Administration Console.

Configure Email Servers to Change Guardian in Non-FIPS Mode

To configure Email servers to Change Guardian running in non-FIPS mode, perform the following steps.

To add email server to Change Guardian:

1. Export the certificate from the respective SMTP server site.

2 Import the certificate using the following command: `/opt/novell/sentinel/jre/bin/keytool -import -alias <appropriate_alias> -keystore /etc/opt/novell/sentinel/config/.activemqkeystore.jks -file <certificate_file_path> -storepass password`.

NOTE: If you have used a custom path for installation, modify the command accordingly.

3 Restart the Change Guardian server using the following command: `rcsentinel restart`.

4 Add new email configuration with STARTTLS protocol using Policy Editor.

5 Create routing rules in Administration Console.

Adding Email Servers to Change Guardian

To add an email server to Change Guardian, perform the following steps.

To add the email server:

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**.

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 Administration Console, you can choose from the notification groups available for that email server. For more information, see “Creating Rules to Send Emails” on page 113.

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 or semicolons, that receive email alerts.
   - **CC** A list of email addresses, separated by commas or semicolons, that receive copies of email alerts.
   - **BCC** A list of email addresses, separated by commas or semicolons, 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.

Creating Rules to Send Emails

To send email messages from within the Administration 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.

To assign email alerts to an event:

1. Log in to the Administration 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. Ensure that you set correct filters to avoid unnecessary flow of emails.

---

10 Configuring Data Federation

The Change Guardian Data Federation feature enables you to search for events, view alerts, and run reports not only on your local Change Guardian server, but also on other Change Guardian servers distributed across the globe.

Overview

The Data Federation feature facilitates searching events, viewing alerts, and reporting event data from local and remote Change Guardian servers. When you are working with multiple servers, you can perform a search or run a report on just one server and have it automatically run a search or report across the selected remote servers. The server on which the search is initiated is referred to as the authorized requestor, and the remote servers are referred to as the data sources or data source servers.

When you run a search or report on the authorized requestor, search queries are sent to each selected data source server. The data source server authenticates the authorized requestor server, using a password that is exchanged during configuration. Event or alert data is returned to the authorized requestor, where it is merged, sorted, and rolled up for presentation. Individual search results display the data source servers from which they were received. The search status for each server is available for viewing and troubleshooting.

Servers

To configure an authorized requestor for data federation, you must first enable data federation on the authorized requestor server.

After you enable data federation, you need to add data source servers to the authorized requestor server. If you know the administrator user name and password for the data source server, you can add the data source server directly from the authorized requestor.

If you do not know the administrator user name and password for a data source server, you can set up the authorized requestor with an opt-in password that allows administrators of data source servers to add their data source servers to the authorized requestor. When you do this, administrators of data source servers do not need to share their user names and passwords with you. You must share the opt-in password with the data source server administrator.

- "Enabling Data Federation" on page 116
- "Using the Administrator Credentials to Add a Data Source Server" on page 116
- "Using the Opt-in Password to Add a Data Source Server" on page 117

Enabling Data Federation

1. Create a role with **Proxy for Authorized Data Requestors** permission. For information on how to configure users and roles, see Configuring Roles and Users.
2. From Administration Console log in as an administrator, click **Integration** > **Change Guardian**
3. Select **Local server and other data sources** in the **Data Sources** section.
4. Do one of the following to add data source servers to your authorized requestor:
   - If you are the administrator of the authorized requestor and you know the administrator user name and password on the data source server, continue with "Using the Administrator Credentials to Add a Data Source Server" on page 116.
   - If you are the administrator of the authorized requestor and you do not know the administrator user name and password on the data source server, you can set an opt-in password to allow administrators of data source servers to add their data source servers to the authorized requestor. Continue with "Using the Opt-in Password to Add a Data Source Server" on page 117.

Using the Administrator Credentials to Add a Data Source Server

If you are the administrator of the authorized requestor and you know the administrator user name and password on the data source server, you can add the data source server while you are logged in to your authorized requestor server.

IMPORTANT: You should ensure that the data source server that you add is able to communicate with the authorized requestor. The data source server should be able to communicate through TCP/IP. The IP address or host name of the data source server must be accessible through firewalls, NATs, etc. You can use the ping command to ensure that there is communication from both ways. If there is a communication failure between the servers, an error is displayed in the extended status page. For more information, see "Managing Search Results" on page 121.

---

1. If you are continuing from "Enabling Data Federation" on page 116, skip to Step 4; otherwise, continue to Step 2.
2. From Administration Console log in as an administrator, click **Integration** > **Change Guardian**
3. Select **Local server and other data sources** in the **Data Sources** section.
4. Click the **Add a data source** link.
5. Specify the following information:

   IP Address/DNS Name: IP address or the DNS name of the data source server.

Port: Port number of the data source server. The default port number is 8443. The data source server and authorized requestor do not need to be on the same port.

User Name: User name to log in to the data source server. This must be a user with administrator privileges.

Password: Password associated with the user name.

6 Click **Login**, then click **Accept** after verifying that the certificate information is correct.

7 Use the following information to configure the data source server:

The Add a data source page displays a lists of the various proxy roles on the data source server.

Name: Specify a descriptive name that you want to give to the data source.

This helps you to easily identify the data source server by a name instead of by its IP address or DNS name.

Search Proxy Role: Select a search proxy role that you want to assign to the authorized requestor.

When the authorized requestor makes search requests to the data source server, the proxy role's security filter is used when performing the search. Only events that pass the proxy role's security filter are returned to the authorized requestor server.

Only roles that have the `Proxy for Authorized Requestors` permission are listed. This permission is required for the data source server to accept and process incoming search requests from the authorized requestor server.

8 Click **OK**.

The server information is listed in the **Data Sources** list.

You can now search events, view event reports, and view alerts from the data source server. For more information, see “Searching for Events” on page 120, “Running Reports” on page 122, and “Viewing Alerts” on page 123 respectively.

Using the Opt-in Password to Add a Data Source Server

In organizations where administrative control of Change Guardian servers is decentralized, it might violate the security policy to share administrator passwords. However, Change Guardian allows you to share a limited-purpose opt-in password to add data source servers, which is more secure than requiring full administrator credentials. If you are not the administrator of the data source server, you can set an opt-in password in the authorized requestor server, then provide the opt-in password to the data source server administrators to allow them to opt in to the authorized requestor server.

When a data source server opts in to the authorized requestor, a message is sent to the authorized requestor server requesting that it be added to the list of data source servers maintained by the authorized requestor server. The request authorizes the authorized requestor to access data on the data source server. The authorized requestor requires an opt-in password to verify that the opt-in request has originated from a valid data source server. During the opt-in process, the authorized requestor and the data source server exchange the appropriate password, which allows the data source server to authenticate the search requests from the authorized requestor.

This procedure is similar to adding a data source server, but it is done from the data source server instead of the authorized requestor server.

- “Setting the Opt-In Password” on page 118
- “Authorizing an Authorized Requestor Server” on page 118

Setting the Opt-In Password

1. Log in to the authorized requestor server as an administrator.
2. Click **Integration** in the toolbar, and then click **Change Guardian**.

   The Data Federation page that is displayed has two sections: **Data Sources** and **Authorized Requestors**.
3. In the **Data Sources** section, select **Local server and other data sources**.
4. Click **Set Opt-in Password**.
5. Specify the opt-in password, then click **Set Password**.
6. Continue with "Authorizing an Authorized Requestor Server" on page 118 to add the data source server to the authorized requestor.

Authorizing an Authorized Requestor Server

1. Log in to the data source server as an administrator.
2. Click **Integration** in the toolbar, and then click **Change Guardian**.

   The Data Federation page that is displayed has two sections: **Data Sources** and **Authorized Requestors**.
3. In the **Authorized Requestors** section, check the **Allow authorized requestors to access data from your server** box.
4. Click the **Add** link.

   The Add authorized requestors page is displayed.
5. Specify the following information:

   IP Address/DNS Name: The IP address or the DNS name of the authorized requestor.

   Port: Port number of the authorized requestor. This is the port number on which the authorized requestor listens for incoming opt-in requests. The default port number is 8443.

   Opt-in Password: The opt-in password that you configured on the authorized requestor. You must obtain this password from the administrator of the authorized requestor.
6. Click **OK**.

   The Confirm Certificate page is displayed.
7. Verify the certificate information, then click **Accept**.

   The Add authorized requestors page is displayed that lists the various proxy roles on the data source servers.
8. In the **Name** field, specify a descriptive name that you want to give to the authorized requestor server.

   This helps you to easily identify the authorized requestor server by a name instead of by its IP address or DNS name.
9. Select a proxy role that you want to assign to the authorized requestor.

   When the authorized requestor makes search requests to the data source server, the proxy role's security filter is used when performing the search. Only events that pass the proxy role's security filter are returned to the authorized requestor.

   Only roles in the data source server that have the `Proxy for Authorized Requestors` permission are listed. This permission is required for the data source server to accept and process incoming search requests from the authorized requestor.
10. Click **OK**.

The authorized requestor is added to Authorized Requestors list and is enabled by default.

The data source server is also added in the Data Sources list in the authorized requestor server. Alternatively, you can click the **Refresh** link to see the data source server in the Data Sources list.

FIPS in Data Federation

This section provides information about configuring distributed search in FIPS 140-2 mode.

Scenario 1: Both the source and the target Change Guardian Servers are in FIPS 140-2 mode

To allow distributed searches across multiple Change Guardian servers running in FIPS 140-2 mode, you need to add the certificates used for secure communication to the FIPS keystore.

1. Log in to the distributed search source computer.
2. Browse to the certificate directory:

   ```
   cd /etc/opt/novell/sentinel/config/
   ```

3. Copy the source certificate (`sentinel.cer`) to a temporary location on the target computer.
4. Import the source certificate into the target server's FIPS keystore.

   For more information about importing the certificate, see "Import certificates into the FIPS Keystore Database:" on page 120.
5. Log in to the distributed search target computer.
6. Browse to the certificate directory:

   ```
   cd /etc/opt/novell/sentinel/config
   ```

7. Copy the target certificate (`sentinel.cer`) to a temporary location on the source computer.
8. Import the target system certificate into the source server's FIPS keystore.
9. Restart Change Guardian service on both the source and target computers: `rcsentinel restart`

Scenario 2: The source Change Guardian Server is in non-FIPS mode and the target Change Guardian Server is in FIPS 140-2 mode

You must convert the Web server keystore on the source computer to the certificate format and then export the certificate to the target computer.

1. Log in to the distributed search source computer.
2. Create the Web server keystore in certificate (`.cer`) format:

   ```
   /opt/novell/sentinel/jdk/jre/bin/keytool -export -alias webserver -keystore /
   etc/opt/novell/sentinel/config/.webserverkeystore.jks -storepass password -
   file <certificate_name.cer>
   ```

3. Copy the certificate to a temporary location on the distributed search target computer.
4. Log in to the distributed search target computer.
5. Import the source certificate into the target server's FIPS keystore.

   For more information about importing the certificate, see "Import certificates into the FIPS Keystore Database:" on page 120.
6. Restart Change Guardian Service service on the target computer:`rcsentinel restart`

Scenario 3: The source Change Guardian Server is in FIPS mode and the target Change Guardian Server is in non-FIPS mode

1. Log in to the distributed search target computer.
2. Create the Web server keystore in certificate (`.cer`) format:

   ```
   /opt/novell/sentinel/jdk/jre/bin/keytool -export -alias webserver -keystore /
   etc/opt/novell/sentinel/config/.webserverkeystore.jks -storepass password -
   file <certificate_name.cer>
   ```

3. Copy the certificate to a temporary location on the distributed search source computer.
4. Import the target certificate into the source server's FIPS keystore.

   For more information about importing the certificate, see "Import certificates into the FIPS Keystore Database:" on page 120.
5. Restart Change Guardian service on the source computer:`rcsentinel restart`

Import certificates into the FIPS Keystore Database:

1. Copy the certificate file to any temporary location on the Change Guardian server or remote Collector Manager.
2. `chown novell:novell /<path to certificate>`
3. `chmod 644 /<path to certificate>`
4. Browse to the Sentinel bin directory. The default location is `/opt/novell/sentinel/bin`.
5. Run the following command to import the certificate into the FIPS keystore database, and then follow the on-screen instructions:.

   ```
   ./convert_to_fips.sh -i <certificate file path>
   ```

6. Enter `yes` or `y` when prompted to restart the Change Guardian server or remote Collector Manager.

Searching for Events

Searching for events in a distributed environment is similar to how you perform a search on your local server, except that you perform the search on the selected data source servers and can also include your local server.

1. Log in to the authorized requestor server as a user with Search Remote Data Sources permission.
2. Click **New Search**.
3. Click the **Data sources** link under the **Search** field.

   A dialog box is displayed that lists the data source servers that you have added, including the local server. The data source servers that are disabled are also displayed, but they are dimmed.
4. Select the check boxes next to the data source servers on which you want to perform a search, then click **OK**.
5. Specify the search criteria in the search field, then click **Search**.

If you do not specify any search criteria, the authorized requestor server runs a default search for all events with severity 0 to 5.

The Search Results page displays the events from the selected data source servers and the local server (if selected). The search results are filtered through the combination of the security filter and permissions of the logged-in user and the security filter and permissions of the search proxy role on the data source servers. For information on the distributed search results, see "Managing Search Results" on page 121.

Managing Search Results

The Search Results page displays the events from the selected data source servers and the local server, based on the search criteria you specified. Each event displays the data source server information from which the event is being retrieved.

You can expand the event results to see the details by clicking the **All** link.

For non-internal events, the **get raw data** link is displayed. You can view the raw data only if your role's security filter is set to view all event data.

NOTE: For search results that come from the data source servers, the role that is used to retrieve raw data is not the role of the logged-in user that is performing the search on the authorized requestor server, but the role that is assigned to the authorized requestor server on the data source server.

You can view the status of the search in the extended status page while a search is in progress as well as when the search has finished. To access the extended status page, click the **Displaying N of M events from X data sources** link that appears at the top of the refinement panel.

The extended status page displays the following information:

- **Data Source Name:** The descriptive name of the data source server. If you did not specify a descriptive name for the data source server, this field displays the IP address or DNS name of the data source server.
- **Events Available:** Indicates the number of events that have actually been retrieved from the data source server. The value is displayed as `N of M events available`, where N is the number of events that have been retrieved so far and M is the total number of events on the data source server that match the search criteria.
- **Retrieval Rate (EPS):** An approximate rate of how fast the events were retrieved from a specific data source server.
- **Status:** Displays the error messages, if any (generally in red). In addition to error messages, this field also displays the status of the search.
  - **Running:** Indicates that the search is still running on the data source server.
  - **Buffering events for display:** Indicates that the search is finished on the data source server, but the authorized requestor server is retrieving events from the data source server and buffering them for display.
  - **Paused buffering events for display:** Indicates that the search is finished on the data source server, and the authorized requestor has paused while retrieving events from the data source. The authorized requestor reads ahead a few pages from the last page that you scrolled down to. When it has buffered enough pages ahead, it pauses so that events are not buffered unnecessarily.
  - **Searching, paused buffering events for display:** This is similar to pausing and buffering events for display, except that the search is not yet complete on the data source server.

- **Done buffering:** Indicates that the search is complete on the data source server, and all of the results are retrieved by the authorized requestor and queued for display.

Viewing Search Activities

You can view the search activities that are being done on the data source server by the authorized requestor server. You can see what queries are being done and how frequently they are being done. Based on the search activity, you might want to assign a more/less restrictive proxy role or even disable access to the data source server.

You can also refine the search activity query. For example, you can change the date range to see what queries have been performed today or yesterday or in the last hour, or you can drill down to see the queries that were made by particular users on the authorized requestor.

1. Log in to the data source server as an administrator.
2. Click **Integration** in the toolbar, and then click **Change Guardian**.

   The Data Federation page that is displayed has two sections: **Data Sources** and **Authorized Requestors**.
3. In the **Authorized Requestors** section, a list of authorized requestor servers is displayed. Click the **Search Activities** link for the authorized requestor server for which you want to view the search activities.

   The search activities page is displayed that lists the audit events that are retrieved from all of the distributed search requests the data source server has received from that particular authorized requestor.

Running Reports

Running reports in a distributed environment is similar to running reports on your local server, except that you select the data source servers from which you want to view the reports while specifying the report parameters.

1. Log in to the authorized requestor sever as a user with Search Remote Data Sources permission.
2. From the Reports section, select the report you want to run, then click **Run**.

   The Run Report page is displayed.
3. Click the **Data sources** link.

   A page is displayed that lists the data source servers that you have added, including the local server. The data source servers that are disabled are also displayed, but they are dimmed.
4. Select the data source servers from which you want to view the reports, then click **OK**.
5. Specify the other parameters for the report.
6. Click **Run**.

   A report results entry is created and listed under the selected report.

Viewing Alerts

Viewing alerts in a distributed environment is similar to viewing alerts from your local server, except that you select the data source servers from which you want to view alerts while creating alert views.

To view alerts from data source servers, you must log in to the authorized requestor server as a user with Search Remote Data Sources permission.

Editing Data Source Server Details

1. From Administration Console log in as an administrator, click **Integration** > **Change Guardian**
2. In the **Data Sources** section, a list of data source servers is displayed under the Data Source Servers list.
3. Click the **Edit** link for the data source server for which you want to modify the details, then edit the information.

   You can edit the name of the data source server and the port number.
4. (Optional) To change the proxy role on the data source server as necessary:
   - **4a** Click **View/Change**.
   - **4b** Log in to the data source server.
   - **4c** Select a proxy role, then click **OK**.
5. Click **Save**.

Troubleshooting

You can perform some basic troubleshooting to ensure that you have successfully configured the authorized requestor for data federation. This section lists the most common issues and the probable causes for these issues.

Permission Denied

After doing a distributed search, check the extended status page to view the search status. If the search is not successful, check the following possible causes:

- The data source server administrator might have disabled data federation on the data source server. To enable data federation on the data source server, see Step 3 in "Authorizing an Authorized Requestor Server" on page 118.

- The data source server administrator might have disabled the authorized requestor server for data federation. Ensure that the authorized requestor server is enabled in the data source server. Fore more information, see “Authorizing an Authorized Requestor Server” on page 118.
- The role that you used for connecting might not have the `Search Data Targets` permission.

Connection Down

- Network issues in your organization.
- Change Guardian servers or Change Guardian services might be down.
- Connection time-out.
- The IP address or the port number of the data source server has changed, but the authorized requestor configuration might not be updated.

Unable to View Raw Data

The Proxy group that is assigned to the authorized requestor might not have the `view all events` permission to view the raw data.

Problems While Adding Data Source

The authorized requestor server and data source server might not be communicating with each other. Ensure that the firewall and NAT are set up properly to allow communication in both directions. Ping both ways to test.

Some Events Are Only Visible from the Local System

You might not be able to view the events from the data source servers for one of the following reasons:

- The trial license might be expired. You must purchase an enterprise license to reactivate this feature to view the events from the data source servers.
- The user who has logged in to the authorized requestor has one set of permissions on the local data such as view all data, view system events, security filter settings, and so on. The search proxy group has another set of permissions, possibly more restrictive. Therefore, certain types of data, such as raw data, system events, and PCI events, might be returned only from the local system and not the data source server.

Cannot Run Reports on the Data Source Servers

The trial license might be expired. You must purchase an enterprise license to reactivate this feature to run the reports from the data source servers.

Different Users Get Different Results

Different users might have different security filters or other permissions and therefore get different results from a distributed search.

Cannot Set the Admin Role as the Search Proxy Role

This is by design, for security reasons. Because the data viewing rights for the admin are unrestricted, it is not desirable to allow the admin role to be the search proxy role.

Error Logs

You can also determine the cause of a search failure by examining the log file on the authorized requestor server. The default location for the log file is `/var/opt/novell/Change Guardian/log`. For example, you might see one of the following messages:

```
Invalid console host name 10.0.0.1

Error sending target request to console host 10.0.0.1

Error getting certificate for console host 10.0.0.1

Authentication credentials in request to opt-in to console 10.0.0.2 were rejected

Request to opt-in to console 10.0.0.2 was not authorized

Error sending target request to console host 10.0.0.1
```

11 Configuring Integrations with Other Software

This section provides information about integrating Change Guardian with the Security Information and Event Management (SIEM) solutions to forward event to enhance event analysis, use Identity Management Systems to get user details, track Active Directory using Directory and Resource Administrator (DRA) as events, and Workflow Automation that triggers a workflow when alerts are generated.

This chapter provides the following information

Integration with SIEM Solutions

Change Guardian and the SIEM solution products such as, Micro Focus Sentinel Enterprise, Splunk Enterprise Security, and ArcSight Enterprise Security Manager are security monitoring solutions. Change Guardian provides focused security for change details and privilege user monitoring, and can forward these specialized change monitoring details to other SIEM solutions for consolidated monitoring, correlations and analysis.

SIEM Product Name	Event Forwarding Mechanism
Sentinel	REST Dispatcher or Syslog Dispatcher
Splunk Enterprise Security	Syslog Dispatcher
ArcSight Enterprise Security Manager	Syslog Dispatcher

In Sentinel you can analyze the change events forwarded by Change Guardian, while the other SIEM solution products use Change Guardian to analyze the data.

To configure event forwarding to other SIEM solution products, see "Configuring Event Destinations" on page 99.

Integrating with Identity Management Solutions

Change Guardian provides an integration framework for AD or IDM to track identities of each user account and what events those identities have performed.

This integration provides functionality on several levels:

- The People Browser provides the ability to look up the following information about a user:
  - Contact information

- Accounts associated with that user
- Most recent authentication events
- Most recent access events
- Most recent permissions changes

- Reports and Correlation rules provide an integrated view of a user's true identity, even across multiple systems on which the user has separate accounts. For example, accounts like `COMPANY\testuser; > cn=testuser,ou=engineering,o=company`, and `TUser@company.com` can be mapped to the actual person who owns the accounts.

By displaying information about the people initiating a given action or people affected by an action, incident response times are improved and behavior-based analysis is enabled.

NOTE: Only administrators can integrate Change Guardian with identity management systems.

Integrating with Active Directory

Change Guardian only provides initiator's user name and the ObjectSID of an event during auditing activities. However, more information is essential to detect and assess risks.

The benefits of Change Guardian integration with AD are as follows:

- Permits the Change Guardian server to retrieve user information from AD and map with associated incoming events.
- Helps map user profiles with attributes in the web console.

These allow you to enrich available information and so better detect and assess risks. Some additional features also include:

- Receive delta values from AD.
- Support for adding additional attributes.
- Support for mapping custom attributes.
- Synchronize users from multiple user containers concurrently.
- Synchronize deleted users.

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.

- "Adding a User Container" on page 129
- "Mapping User Profile Fields" on page 129

Using the Administration 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 Administration Console, click **Integration**.
2. Click **AD Accounts**.

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 Administration Console, click **Integration > AD Accounts > Add User Container**.
2. Provide the appropriate information for the user container you want to synchronize.

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 Administration Console, click **Integration**> **AD Accounts**> **User Profile Mapping**.

Integration with Identity Manager

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

To view user identity details:

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.

For more information about integrating identity information with Change Guardian events, see "Integrating Identity Information" in the *"Sentinel Administration Guide"*.

Searching and Viewing Identity Information

To search and view identity information, see Searching and Viewing User Identities in the *"Change Guardian User Guide".*

Integration with Workflow Automation

Change Guardian allows communication with Workflow Automation (formerly known as NetIQ Aegis) to receive Change Guardian alerts and initiate a workflow. If an alert received from Change Guardian matches a trigger associated with a workflow, Workflow Automation initiates a work item.

For more information about working with Workflow Automation and Change Guardian, see "*Aegis Adapter for Sentinel*."

Integration with Directory Resource Administrator

Change Guardian provides enhanced user monitoring in conjunction with DRA. It provides solution to control, manage and monitor the Active Directory environments.

Change Guardian server captures the unmanaged changes on DRA and displays the *actual* user name (end-user who logged in to DRA) in the event list on the Administration Console. As an auditor you can monitor the AD audit logs or events from DRA, and view the corresponding actual user name on the Change Guardian event list.

12 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 allows you restore the data at any time on the Change Guardian server.

NOTE: To ensure compatibility you must restore backed up data to the same version of Change Guardian, use the same computer (IP address and Hostname match) you used to create the backup and ensure that the Install Configuration or custom path (if any) and FIPS configuration also match the original.

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

- **System Failure**: If system fails, 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**: If data is lost, 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.

- “Parameters for the Backup and Restore Utility Script” on page 132
- “Running the Backup and Restore Utility Script” on page 133
- “Restoring Data” on page 135

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 12-1 *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.

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 novelluser.

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 12-1. 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/<my_full_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/<my_full_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/ <my_full_backup>.tar.gz`	Restores the data from the specified filename. **NOTE:** To successfully restore the data from backup, ensure that the backup file ownership is set to user `novell` and group `novell`.
`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 “Restoring Data” on page 135.

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 Administration Console. 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.

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 Administration Console. In the Search results, click **All** for any local event.

Viewing Event Data Available for Restoration

1. Log in to the Administration Console 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 136 to restore the event data.

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 135.

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 in 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”.

Configuring Retention Period

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.

13 Upgrading Change Guardian

This chapter provides information about upgrading Change Guardian.

Upgrade Checklist

You can upgrade to Change Guardian 5.2 from Change Guardian 5.1.1. If you have Change Guardian 5.1, upgrade first to Change Guardian 5.1.1.

You must upgrade both the Change Guardian server and the Policy Editor. The Change Guardian Agent for Windows are backward compatible.

NOTE: TLS 1.0 is not disabled by default in upgrade installations of the Change Guardian server, agents, and Policy Editor components in order to preserve backward compatibility with components that might not be upgraded yet. Once you upgrade all the components to the latest released versions, you can disable TLS 1.0. For more information, see “Prerequisites of Disabling TLS 1.0” on page 47.

Use the following checklist to upgrade your Change Guardian installation:

Table 13-1 *Upgrade Checklist*

	Tasks	See
❒	Ensure that the computers on which you install Change Guardian components meet the specified requirements. **NOTE:** Change Guardian is not supported if the operating system is in FIPS mode. Ensure your operating system is not in FIPS mode before you upgrade.	Supported Platforms on the System Requirements page.
❒	If you need to upgrade the operating system on the Change Guardian server, understand the recommended order for the upgrade.	“Upgrading the Appliance Installation” on page 142
❒	Review the supported operating system release notes to understand the known issues.	SUSE Release Notes

	Tasks	See
❒	Review the Change Guardian release notes to see new functionality and understand the known issues.	Change Guardian 5.2 Release Notes
❒	Upgrade the Change Guardian server.	◆ "Upgrading a Traditional Installation" on page 140 ◆ "Upgrading the Appliance Installation" on page 142
❒	Upgrade the Change Guardian components.	◆ "Upgrading Components" on page 144 ◆ "Upgrading Change Guardian Agent for Windows" on page 144 ◆ For information on how to upgrade Security Agent for UNIX remotely, refer to Security Agent for UNIX documentation.

Prerequisite

Ensure that the latest patch of Microsoft Windows is running on the system running the Change Guardian Agent for Windows.

Upgrading a Traditional Installation

You can upgrade the following installation types:

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

Following sections provide more information about upgrading.

- "Upgrading Change Guardian" on page 140
- "Upgrading the Operating System" on page 141

Upgrading Change Guardian

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

To upgrade the Change Guardian Server in a traditional installation:

1. Back up all your information using the `backup_util.sh` script. For information about using the backup utility, see Chapter 12, "Backing Up and Restoring Data," on page 131.
2. Download the latest installer from the Micro Focus Patch Finder website and copy it to the server. 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 Change Guardian server you want to upgrade.

4 Specify the following command to extract the install files from the tar file:

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

5 Change to the directory where the install file was extracted.

6 Specify the following command to upgrade Change Guardian:

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

7 (Conditional) If you want to upgrade from a custom path, specify the following command:

```
./install-changeguardian.sh --location=<custom_CG_directory_path>
```

NOTE: You can only upgrade from a custom path used for the original installation and has 0755 permissions.

8 To proceed with a language of your choice, select the number next to the language.

9 If there are changes to the end user license agreement, read and accept the changes.

10 Specify `yes` to approve the upgrade.

11 (Conditional) If your system does not meet the recommended disk space,

12 Verify whether the Administration Console can connect to the server by specifying the following URL in your web browser:

`https://IP_Address_Change_Guardian_server:8443`

Based on your requirement, you must perform the post-upgrade tasks. For more information, see "Post Upgrade Configuration" on page 145.

Upgrading the Operating System

Follow the steps below to upgrade the operating system:

1 Stop Change Guardian services:

```
/opt/netiq/cg/scripts/cg_services.sh stop
```

2 (Conditional) If Change Guardian was in FIPS mode before the operating system upgrade, NSS database files must be manually upgraded by running the following command:

```
certutil -K -d sql:/etc/opt/novell/sentinel/3rdparty/nss -X
```

Follow the on-screen instructions to upgrade the NSS database.

Give full permissions to `novell` user for the following files in folder `/etc/opt/novell/sentinel/3rdparty/nss`:

```
cert9.db
key4.db
pkcs11.txt
```

3 Upgrade the operating system.

4 (Conditional) If you use Mozilla Network Security Services (NSS) 3.29 and later, two dependent RPM files `libfreebl3-hmac` and `libsoftokn3-hmac` are not installed.

Manually install the following RPM files: `libfreebl3-hmac` and `libsoftokn3-hmac`.

5 (Conditional) During the upgrade process, SLES renames the `/etc/sysctl.conf` file to `/etc/sysctl.conf.rpmsave` as a back up and creates a new `/etc/sysctl.conf` file. Once you upgrade, verify if the file `rpmsave` has entries for parameters `net.core.wmem_max` and `vm.max_map_count`.

If either of the parameters are not present, add the following parameters to the `sysctl.conf` file as follows:

```
net.core.wmem_max = 67108864
# Added by sentinel vm.max_map_count: 65530
vm.max_map_count = 262144
```

6 (Conditional) For RHEL 7.x, run the following command to check whether there are any errors in the RPM database: `rpm -qa --dbpath <install_location>/rpm | grep novell`

Example: `# rpm -qa --dbpath /custom/rpm | grep novell`

- If there are any errors, run the following command to fix the errors:

  `rpm --rebuilddb --dbpath <install_location>/rpm`

  Example: # rpm --rebuilddb --dbpath /custom/rpm

- Run the command mentioned in Step 6 to ensure that there are no errors.

NOTE: 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 Administration Console until you upgrade the Change Guardian server.

Upgrading the Appliance Installation

This section provides information about upgrading to Change Guardian Appliance 5.2.

Configuring Appliance for Upgrade

To configure appliance for upgrade, perform the following steps:

To upgrade from 5.1 to 5.2

1 Download the following file to the Change Guardian server: `changeguardian_appliance_configuration_utility_5100-32.tar.gz` from Micro Focus Downloads.

2 Extract the file by running the following command: `tar -xvf changeguardian_appliance_configuration_utility_5100-32.tar.gz`.

3 Use the `cd` command to change to the directory where you extracted the utility.

4 To configure the appliance, run the following script:

`./cg5100-appliance_configuration.sh`

This script configures the required packages to manage the appliance.

WARNING: Do not run this script remotely as it involves network reconfiguration, which in turn might interrupt the configuration.

5 Go to “Applying the Updates” on page 143.

To upgrade from 5.1.1 to 5.2

To upgrade from 5.1.1 to 5.2 go to “Applying the Updates” on page 143.

Applying the Updates

The following are the two methods in which you can apply the updates:

- “Applying Updates Using the Change Guardian Appliance Console” on page 143
- “Applying Updates Using Zypper” on page 143

Further, in secured environments where the appliance must run without direct Internet access, you may contact Technical Support.

Following sections provide more information about applying updates.

Applying Updates Using the Change Guardian Appliance Console

1 Log in to the following URL to register to the Change Guardian appliance update channel: https://IP_Address_Change_Guardian_server:9443.

2 Use the appliance update channel to receive Change Guardian and operating system updates.

For more information, see “Applying the Updates” on page 143.

3 Log in to the Change Guardian Appliance Console as the `vaadmin` or `root` user.

4 Click **Online Update**.

5 Select **Needed Patches** from the drop-down list and click **Update Now**.

6 Select **Needed Patches** from the drop-down list to ensure that there are no pending updates.

Applying Updates Using Zypper

You can upgrade Change Guardian by using Zypper. Zypper is a command line package manager that allows you to perform an interactive upgrade of appliance. In instances where user interaction is required to complete the upgrade, such as an end user license agreement update, you must use Zypper to upgrade the Change Guardian appliance.

For information about which methods of upgrade are supported for a release, see the Release Notes.

NOTE: Ensure you apply updates only after upgrading Change Guardian, the operating system and then running the appliance configuration utility.

To update the appliance using zypper, perform the following steps:

1 Log in to the server Command Line Interface as `root`.

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

3 Install the Zypper updates by running the command `zypper patch`.

WARNING: Always use the `zypper patch` command to 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.

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

5 Rerun the command `zypper patch` to install the appliance updates.

For more information, see the Zypper Cheat Sheet.

Upgrading Components

You have to upgrade the following after upgrading Change Guardian:

Upgrading Policy Editor

The procedures for upgrading the Policy Editor is the same as the procedure for installing it. For more information, see “Installing Policy Editor” on page 32.

Upgrading Change Guardian Agent for Windows

You can upgrade Change Guardian Agent for Windows manually or by using Agent Manager.

NOTE: The procedures for upgrading the Change Guardian Agent for Windows manually is the same as the procedure for installing them, except that you do not need to repeat the process of adding assets to Agent Manager. You must not rename the default `.msi` installer package. For more information, see “Manual Installation” on page 34.

To upgrade using Agent Manager:

1 From the assets list, select the an agent which you want to upgrade. You can select multiple computers if Agent Manager can use the same credentials to connect to the computers.

2 Provide credentials for an account that can connect to the computer and click **Next**.

The account must be the local administrator account or a domain account in the Local Administrators group.

3 Click **Manage Installation**, and then select **Upgrade**.

4 Perform the following steps:

4a For the agent version, select **Change Guardian Agent for Windows *Agent Version***, where *Agent Version* is the version of the agent you want to deploy.

4b Click **Start Upgrade**.

Applying Updates to Change Guardian Components

Micro Focus might occasionally provide bug fixes and improvements to the Change Guardian Agent for Windows, the Security Agent for UNIX, or Policy Editor. You can use the Agent Manager to upload the agent packages or the Policy Editor patch for deployment in your environment.

To apply the patch:

1 Download the patch from the Micro Focus Patch Finder.

2 Log in to Agent Manager.

3 Go to **All Assets** > **Manage Installation** > **Upload Package**.

This uploads the package to Change Guardian server.

4 To upgrade the agents or download Policy Editor, log in to Agent Manager on the machine running the agent or Policy Editor.

5 (Conditional) **All Assets** > **Manage Installation** > **Download Package**, then upgrade.

For more information about upgrading, see Upgrade Policy Editor.

6 (Conditional) To upgrade the agents, go to **Manage Installation** > **Upgrade Agents**.

Adding Application License after Upgrade

You must import license keys for each module you want to use.

To import and assign a license:

1 Login to **Policy Editor**.

2 Click **Module Manager**.

3 Click the given remote end point in the Licenses section of the right hand panel.

4 Click **Import License Key**.

5 Browse and select the module license file.

6 Click **Import**.

Post Upgrade Configuration

Change Guardian now provides the `chg_keystore_pass.sh` script that allows you to change the keystore passwords. As a security best practice, you must change the keystore passwords immediately after upgrading Change Guardian.

NOTE: You need not perform this procedure if Change Guardian server is in FIPS mode.

To change the keystore passwords:

1 Log in to the Change Guardian server as the `novell` user.

2 Go to the `/opt/novell/sentinel/bin` directory.

3 Run the `chg_keystore_pass.sh` script and follow the on-screen prompts to change the keystore passwords.

Verifying the Upgrade

You can determine whether the installation is successful by performing either of the following:

- Ensure the server is running: `netstat -an | grep LISTEN | grep 8443`
- Verify that the latest packages are installed: `rpm -qa | grep -i ncg`
- To access the Change Guardian dashboard, specify the following URL in your web browser:

  `https://IP_Address_Change_Guardian_server:8443/cg-main-ui/`

A Appendices

This chapter provides information about the following sections:

Uninstalling Change Guardian

Uninstallation Checklist

Use the following checklist to uninstall Change Guardia:

- Uninstall the following components before you uninstall Change Guardian:
  - Change Guardian Agent for Windows and Security Agent for UNIX using Agent Manager
  - Policy Editor
- Complete the post-uninstallation tasks to verify the Change Guardian uninstallation.

Uninstalling Change Guardian Agent for Windows

You can uninstall the Change Guardian Agent for Windows in the following ways:

Task	See
Uninstall the components.	“Uninstalling Change Guardian Agent for Windows” on page 147 “Uninstalling the Security Agent for UNIX” on page 148 “Uninstalling Policy Editor” on page 148
Uninstall Change Guardian.	“Uninstalling Change Guardian” on page 148
Perform the post-uninstallation steps.	“Post-Uninstallation Tasks” on page 149

- “Remote Uninstallation Using Agent Manager” on page 148
- “Manual Uninstallation” on page 148

Remote Uninstallation Using Agent Manager

Use the following steps to uninstall the agent using Agent Manager:

1. Log in as `administrator` to the Change Guardian server.
2. From Administration Console, click **Integration** > **Agent Manager**.
3. Select the assets from which you want to uninstall the agent.
4. Select **Manage Installation** > **Uninstall Agents**.
5. Click **Start Uninstall**.

Manual Uninstallation

Use the following steps to uninstall the agent:

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

Uninstalling the Security Agent for UNIX

For information about remote uninstallation of Security Agent for UNIX, see *Security Agent for UNIX* documentation.

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**.

Uninstalling Change Guardian

To uninstall the Change Guardian server:

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

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.

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.

Collecting Agent Logs using Agent Manager

You can use Agent Manger to collect logs from both Change Guardian Agent for Windows and Security Agent for UNIX. You must install the agent using Agent Manager to be able to collect the agent logs.

You cannot set debug levels to agent log collection. The logs are collected based on whatever debug level is set in the agent.

To collect agent logs:

1 In Agent Manager, select the agent under **All Assets**.

2 Click **Manage Installation** > **Collect Agent Logs** > **Start Log Collection**.

3 In the **Completed Tasks** tab, click **Download Agent Logs**.

NOTE: You can download a log only once. For an agent, you can download the log that you collected last. The previously collected logs are overwritten every time you click **Collect Agent Logs** for that agent.

Increasing Data Partition Size

You can increase the data partition to suit the sizing need of Change Guardian server:

To increase the partition size:

1 Add a hard disk to the virtual machine.

2 Stop the Change Guardian services by running the following command: `rcsentinel stop`

3 Run the following command to list the partition that was added: `fdisk -l`

4. Format the new disk to ext3 file system by running the following command: `mkfs.ext3 /dev/<partition1>`
5. Create a temporary directory `/tmp/new` to copy files from `/var` or `/opt`.
6. Mount new partition to the temporary directory by running the following command: `mount /dev/<partition1> /tmp/new`
7. Move the data directory to the newly created directory. For example: `mv /var/opt/* /tmp/new`
8. Unmount the temporary directory by running the command: `umount /tmp/new/`
9. Mount the new partition to /var/opt/ by running the command: `mount /dev/partition1 /var/opt/`
10. Confirm that the data partition `/var/opt` is mounted by running the command: mount
11. Verify that the data partition `/var/opt` has moved to the new partition by running the command: `df -h`

Search Query Syntax

Change Guardian uses the Lucene query language for searching events. This section provides an overview of how to use the Lucene query language to perform searches in Change Guardian. For more advanced features, see Apache Lucene - Query Parser Syntax.

For information on the event fields in Change Guardian, click **Tips** on the top right corner in the Administration Console. A table is displayed that lists the event names and their IDs.

Basic Search Query

A basic query is a search for a value on a field. The syntax is as follows:

`msg:<value>`

The field name (msg) is separated from the value by a colon.

For example, to search for a phrase that includes the word “authentication,” you can specify the search query as follows:

```
msg:authentication
```

Or, to search for events of severity 5, you can specify the search query as follows:

```
sev:5
```

If the value has spaces or other delimiters in it, you should use quotation marks. For example:

```
msg:"value with spaces"
```

Change Guardian classifies event fields as either tokenized fields or non-tokenized fields. A tokenized field is indexed and is searched differently than a non-tokenized field.

Case Insensitivity

Indexing and searching in Change Guardian is not case-sensitive. For example, the following queries are all equivalent:

```
msg:AdMin
msg:admin
msg:ADMIN
```

Special Characters

If you include special characters as part of a search, the special characters must be escaped. These characters are as follows:

```
+ - && || ! ( ) { } [ ] ^ " ~ * ? : \ /
```

Use “ \” before the character you want to escape. For example, to search for ISO/IEC_27002:2005 in the rv145 (Tag) field, use the following query:

```
rv145:ISO\/IEC_27002\:2005
```

You can also use quotation marks around the query:

```
rv145:"ISO/IEC_27002:2005"
```

If the value contains quotation marks, you must escape it by using the “\” character instead of quotation marks. For example, to search for “system “mail” service” in the `initiatorservicename` field, you must specify the query as follows:

```
sp:"system \"mail\" service"
```

For more information on quoting wildcard characters, see “Quoted Wildcards” on page 156.

Operators

Lucene supports AND, OR, and NOT Boolean operators, which allow words to be combined. Boolean operators must be always capitalized.

OR Operator

The OR operator is the default conjunction operator. If there is no Boolean operator between two clauses, the OR operator is used. The OR operator links two clauses and finds a matching event if either of the clauses is satisfied. The symbol || can be used in place of the word OR. For example, consider the following query:

```
sun:admin OR dun:admin
```

This query finds events whose initiator username or target username is “admin.” The following query produces the same result because OR is used by default:

```
sun:admin dun:admin
```

AND Operator

The AND operator links two clauses and finds a matching event only if both clauses are satisfied. The symbol && can be used in place of the word AND. For example, consider the following query:

```
sun:admin AND dun:tester
```

This query finds events whose initiator username is admin and the target username is tester.

NOT Operator

The NOT operator excludes events that match the clause after the NOT. The symbol ! can be used in place of the word NOT. For example, consider the following query:

```
sev:[0 TO 5] NOT st:I NOT st:A NOT st:P
```

This query matches all events whose severity is between 0 and 5, but excludes those whose sensor type is I (internal), A (audit), or P (performance); that is, it excludes Change Guardian internal events.

The NOT operator cannot be used by itself because it is a way to exclude events from a set that has been found by other search terms. For example, consider the following query:

```
NOT st:I NOT st:A NOT st:P
```

This query might seem like it should return all events where the sensor type is not I, A, or P. However, it is an invalid query because a query cannot begin with the NOT operator.

Operator Precedence

Parentheses can be used in the usual way to change operator precedence. They can be nested to any depth, as shown in the following examples:

```
(sun:admin OR dun:admin) AND (sip:10.0.0.1 OR sip:10.0.0.2)
```

```
((sun:admin OR dun:admin) AND (sip:10.0.0.1 OR sip:10.0.0.2)) OR (msg:user AND
evt:authentication)
```

The Default Search Field

Lucene uses a default search field, which is the field that is searched if no field is specified. In Change Guardian, `_data` is the default search field. By default, the default search field is a concatenation of the following event fields:

```
evt,msg,sun,iuid,dun,tuid,sip,sp,dip,dp,rv42,shn,rv35,rv41,dhn,rv45,obsip,sn,obsdo
m,obssvcname,ttd,ttn,rv36,fn,ei,rt1,rv43,rv40,isvcc
```

The default search field is indexed and searched as a tokenized field. The result is that you can search for words that might appear in any event field.

You can also customize the set of event fields that are concatenated in the default search field by adding the `indexedlog.datafield.ids` property in the `configuration.properties` file.

For example, suppose you have two non-tokenized fields in an event, sun (initiatorusername) and dun (targetusername). The sun field has the following value:

```
report-administrator
```

The dun field has the following value:

```
system-tester
```

The _data field contains the concatenation of these fields separated by a single space character:

```
report-administrator system-tester
```

Because the _data field is a tokenized field, the words “report,” “administrator,” “system,” and “tester” are indexed and searchable. The following queries would find this event:

```
report
```

```
_data:report
```

```
report-administrator
```

```
_data:report-administrator
```

```
report tester
```

In addition, the following queries also find this event:

```
sun:report-administrator
```

```
dun:system-tester
```

Tokenized Fields

Fields that are classified as tokenized fields are parsed into individual words for indexing. Therefore, a search occurs only on words within the field value. Characters that are considered to be word delimiters are not searchable, nor are words that are considered to be stop words. Lucene removes extremely common words to save disk space and speed up searching. These words are ignored in search filters. Currently, the following stop words are removed:

- a
- an
- and
- are
- as
- at
- be
- but
- by
- for
- if

- in
- into
- is
- it
- no
- not
- of
- on
- or
- such
- that
- the
- their
- then
- there
- these
- they
- this
- to
- was
- will
- with

When it does a search, Lucene examines all of the words in a field and tries to match words in the search value. For example, suppose that you specify a search for messages containing the following value:

```
msg:"user-authentication failed on the server"
```

The words that are parsed within this value are “user,” “authentication,” “failed,” and “server.” These are the only search words that would match this value. “On” and “the” are omitted because they are stop words.

The value has the hyphen character (-) between some words. Hyphens are treated as word delimiters, so Lucene does not search for hyphens. Consider, the following query:

```
msg:"user-authentication"
```

The results might not be exactly what you expect. The query search value matches the value, but not because it is matching the hyphen. It matches because Lucene first parses the words in the search value and identifies the words “user” and “authentication.” Lucene then matches those words against values that have the words “user” and “authentication” with no intervening words in between. This query would also match the following value, even though there is no hyphen between “user” and “authentication”:

```
user authentication has failed on the server
```

Consider the following query:

```
msg:"failed on server"
```

This query has the stop word, "on," which is ignored. However, the stop word does affect the relative positioning that is expected to be between words when evaluating a value to see if it matches. The “failed on server” search matches any phrase where the words “failed” and “server” are separated by exactly one word. It does not matter what the word is because the separating word is a stop word and is ignored. Thus, the above query would match all of the following:

```
failed on server
```

```
failed-on server
```

```
failed a server
```

```
failed-a-server
```

Proximity indicators created by using the ~ character followed by a value, make this more complicated. The query dictates an expected distance between words. In the “failed on server” query, the expected distance between “failed” and “server” is one word. The proximity indicator specifies how much variance there can be from the expected distance. For example, consider the following query, where a proximity indicator of one (~1) is specified:

```
msg:"failed on server"~1
```

This query indicates that the distance between “failed” and “server” could be plus or minus one from the expected distance, which is one because of the stop word “on.” Thus, the distance could be 1, 1-1 (0), or 1+1 (2). Thus, all of the following would match:

```
failed on server
```

```
failed on the server
```

```
failed finance server
```

As of Lucene version 3.1, word parsing is done according to word break rules outlined in the Unicode Text Segmentation algorithm. For more information, see Unicode Text Segmentation.

For information on tokenized fields in Change Guardian, in the Administration Console click **Tips** on the top right corner of the Administration Console. A table is displayed that lists all the event fields and whether an event field is searchable or not.

Non-Tokenized Fields

Fields that are classified as non-tokenized fields are parsed fully for indexing. Thus, a search occurs on full field values. For example, to search events whose initiatoruserfullname (iufname) field has the value “Bob White”, you must specify the query as follows:

```
iufname:"Bob White"
```

Wildcards in Search Queries

Change Guardian supports wildcards in search values but not in regular expressions:

- The asterisk (*) matches zero or more characters.
- The questions mark (?) matches any one character.

For example:

- **adm*test:** Matches admtest, ADMTEST, admintest, adMINtEst (note the lack of case sensitivity).

- **adm?test:** Matches adm1test and AdMatest. Does not match admtest or ADMINTEST because it must have exactly one character between "adm" and "test."

- “Wildcards in Tokenized Fields” on page 156
- “Quoted Wildcards” on page 156
- “Leading Wildcards” on page 157

Wildcards in Tokenized Fields

Wildcards are applied differently to tokenized fields and non-tokenized fields. Wildcards for tokenized fields match only words that were parsed from the value and not the entire value. For example, if you specify the search query `msg:authentication*failed` to search for the message `The user authentication has failed on the server`, it does not return the events with this message. This is because “*” does not match anything between “authentication” and “failed.” However, it matches any words that begin with “authentication” and end with “failed.” For example, it returns results if any of the following words are used: “authenticationhasfailed,” “authenticationuserfailed,” and “authenticationserverfailed.” For tokenized fields, all matching that uses wildcard searches is done on the words within the value and not on the full value.

Quoted Wildcards

Tokenized Fields

When wildcards are quoted, they are not treated as wildcards, but as word delimiters. For example, consider the following query:

```
msg:"user* fail*"
```

The search value "`user* fail*`" is parsed into two words, “user” and “fail.” The semantic is "find any event where the `msg` field contains “user” AND “fail” words in that order, and there are no intervening words between them.” Thus, it does not match the following value:

```
The user authentication has failed on the server.
```

This is because the wildcard is not treated as a wildcard but as a word delimiter.

Non-Tokenized Fields

When wildcards are quoted, they are treated as literal characters to search. For example, if the query is: `sun:"adm*,"` it returns the following values:

```
adm*
```

```
ADM* (case-insensitive)
```

The query does not return the following values:

```
admin
```

```
ADMIN
```

Leading Wildcards

Leading wildcards are not valid in searches because Lucene does not allow the * or ? characters to be the first character of a search value. For example, the following queries are invalid:

- **sun:*adm*** The semantic is “find any event whose initiator username value contains the letters a, d, and m in sequence.“
- **sun:*tester** The semantic is “find any event whose initiatorusername value ends with “tester.”
- **sun:*** The semantic is “find any event whose initiator username field is non-empty.”

  Because this is an important type of query, Change Guardian provides an alternative way to accomplish this. For more information, see “The notnull Query” on page 157.

The notnull Query

You might need to find events where some field is present, or non-empty. For example, to find all events that have a value in the sun field, you can specify the query as `sun:*`

The query does not return the expected results because Lucene does not support wildcards to be the first character of a search value. However, Change Guardian provides an alternate solution. For every event, Change Guardian creates a special field called notnull. The notnull field is a list of all fields in the event that are not null (not empty). For example, if there is an event that has values in the evt, msg, sun, and xdasid fields, the notnull field contains the following value:

```
evt msg sun xdasid
```

The notnull field is a tokenized field, so the following kinds of queries are possible:

- **notnull:sun** Finds all events whose sun field has a value.
- **notnull:xdas*** Finds all events where any field beginning with the name "xdas" has a value.

When a `notnull` field is added in Lucene, creating, indexing, and storing this field adds a cost to processing each event as CPU needs to create and index the field and it also requires additional storage space. If you want to disable storing the list of non-empty fields in the `notnull` field, set the following property in the `/etc/opt/novell/sentinel/config/configuration.properties` file:

```
indexedlog.storenotnull=false
```

Save the file and restart the Change Guardian server. All events received after this property was set do not have a `notnull`field associated.

NOTE: If you disable the `notnull` field, do not use the `notnull` field in search filters, rule filters, or policy filters because the results might be incorrect and unpredictable.

Tags in Search Queries

The Tag field (rv145) is a tokenized field that has special parsing rules for words. The parsing rules enable you to search on tags that include non-alphanumeric characters. However, the only word delimiters are white space characters such as the blank and the tab. This is because tags do not include white space in their names. For example, the following queries find the event if the event is tagged with the ISO/IEC_27002:2005 tag and the NIST_800-53 tag:

```
rv145:"ISO/IEC_27002:2005"
```

```
rv145:"iso/iec_27002:2005"
```

```
rv145:"ISO/IEC_27002*"

rv145:nist_*
```

The slash (/), hyphen (-), and colon (:) characters are significant in the search value because, unlike other tokenized fields, the parsing rules for rv145 do not treat them as a word delimiter. Also, the search is not case sensitive.

The following queries would not find the event:

```
rv145:"ISO IEC_27002 2005"

rv145:"iso *"
```

Regular Expression Queries

Regular expression queries allow you to search events that match a pattern. These queries must be enclosed in quotation marks (“ “) and forward slash (/). For example, to search for an initiator user name that ends with the character "a”, you can specify the search query as follows:

```
sun:"/.*a/"
```

If you need to include special characters in your query, you must escape special characters by preceding them with the backslash (\) character. For example, to search for an initiator user name that ends with the character “$”, you can specify the search query as follows:

```
sun:"/.*\$/"
```

For more information about using special characters, see “Special Characters” on page 151.

NOTE: Regular expression queries utilize significantly more system resources than other kinds of queries because they are unable to leverage the more efficient data structures available in the index. Executing regular expression queries take longer than other kinds of queries and potentially pull system resources from other components of the system. Therefore, use regular expression queries carefully and narrow the breadth of the search as much as possible by using time range and non-regular expression criteria terms.

Range Queries

Range queries allow you to find events where a field value is between a lower bound and an upper bound. Range queries can be inclusive or exclusive of the upper and lower bounds. Whether a particular value falls in the specified range is based on lexicographic character sorting. Inclusive ranges are denoted by square brackets []. Exclusive ranges are denoted by curly brackets {}.

For example, consider the following query:

```
sun:[admin TO tester]
```

This query finds events whose sun field has values between admin and tester, inclusive. Note that "TO" is capitalized.

However, if you change the query as follows:

```
sun:{admin TO tester}
```

The query now finds all events whose sun field is between admin and tester, not including admin and tester.

Some event fields such as sev and xdasid are numeric. In Change Guardian, range queries on numeric fields are based on numeric sorting and not on lexicographic character sorting. For example, consider the following query:

```
xdasid:[1 TO 7]
```

This query returns events whose xdasid value is 1, 2, 3, 4, 5, 6, or 7. If the range evaluation was based on lexicographic sorting, it would incorrectly match 10, 101, 100001, 200, and so on.

IP Addresses Query

There are several extensions that Change Guardian has implemented for searching on IP addresses. Specifically, there are a number of convenient ways to specify IP address ranges. These are explained in the following sections:

- "CIDR Notation" on page 159
- "Wildcards in IP Addresses" on page 159

CIDR Notation

Change Guardian supports the Classless Inter-Domain Routing (CIDR) notation as a search value for IP address fields such as sip (initiator IP) and dip (target IP) for specifying an IP address range. The notation uses a combination of an IP address and a mask, as follows:

```
"xxx.xxx.xxx.xxx/n"
```

In this notation, n is the number of high order bits in the value to match. For example, consider the following query:

```
sip:"10.0.0.0/24"
```

This query returns events whose sip field is an IPv4 address ranging from 10.0.0.0 to 10.0.0.255.

The same notation works for IPv6 addresses. For example, consider the following query:

```
sip:"2001:DB8::/48"
```

This query returns events whose sip field is an IPv6 address ranging from 2001:DB8:: to 2001:DB8:0:FFFF:FFFF:FFFF:FFFF:FFFF.

Wildcards in IP Addresses

You can use only the asterisk character (*) in the IP address search values to specify ranges of IP addresses. You cannot use the question mark (?) character.

In IPv4 addresses, an asterisk (*) can be used at any of the positions in the quad format. In IPv6 addresses, an asterisk (*) can be used between colons to specify a 16-bit segment. For example, all of the following queries are valid on the sip field:

```
sip:10.*.80.16

sip:10.02.*.*

sip:10.*.80.*

sip:"CAFE:*::FEED"

sip:"CAFE:*:FADE:*::FEED"
```

If an asterisk (*) is used in one of the quad positions in an IPv4 address or between colons in an IPv6 address, it cannot be combined with other digits. For example, all of the following queries are invalid:

```
sip:10.*7.80.16

sip:10.10*.80.16

sip:"CAFE:FA*::FEED"

sip:"CAFE:*DE::FEED"
```

Because the question mark (?) is not allowed, the following queries are invalid:

```
sip:10.10?.80.16

sip:10.?.80.16

sip:"CAFE:FA??::FEED"

sip:"CAFE:??DE::FEED"
```

Change Guardian Appliance goes to Emergency mode while rebooting

Rebooting the Change Guardian 5.2 Appliance in Hyper-V causes it to go into emergency mode. This occurs because the operating system modifies the disk UUID during installation. Perform the following steps to overcome this:

1. Login to the Change Guardian 5.2 Appliance in emergency mode with root credentials.
2. Run the command `ls -l /dev/disk/by-id/` and note the actual UUID of the disk.
3. Run the command `cat` for each of the following files to identify the disk UUID entries therein:
   - **/etc/fstab**
   - **/etc/default/grub**
   - **/boot/grub2/grub.cfg**
4. Compare the actual disk UUID entries in /dev/disk/by-id for the SCSI partitions with those in each of the above files.
5. If the disk UUIDs in each of locations do not match the actual values, you must manually replace the incorrect values with actual values.

Example A-1 *Modifying Disk UUIDs*

If the UUID entry in the `fstab, grub or grub.cfg` files is `14d53465420202020f21b50e22267274c823e145500a372b7`, but the UUID on disk is `360022480f21b50e22267145500a372b7`, there is a mismatch which you must manually correct.

Therefore, once the UUID entry is replaced with correct values in the `fstab, grub and grub.cfg` files respectively, the entries therein read as below:

- **/etc/fstab**

  /dev/disk/by-id/scsi-`360022480f21b50e22267145500a372b7`-part1 / ext3 acl 1 1

- **/etc/default/grub**

  GRUB_CMDLINE_LINUX=" root=/dev/disk/by-id/scsi-`360022480f21b50e22267145500a372b7`-part1 nomodeset quiet"

- **/boot/grub2/grub.cfg**

  linux /boot/vmlinuz-4.4.131-94.29-default root=UUID=ace9acb3-ac2b-47f0-960d-5b7cd5b51b47 root=/dev/disk/by-id/scsi-360022480f21b50e22267145500a372b7-part1 nomodeset quiet

6 Reboot the VM.

7 The SCSI disk partition UUIDs are detected correctly and the appliance boots normally.

Troubleshooting

This section contains some of the issues that might occur during installing or using Change Guardian, along with the actions to work around the issues.

Administration Console is Blank on Internet Explorer After Logging in

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

1 Navigate to **Tools** > **Internet Options** > **Security** and set the security level to **Medium-high**.

2 Make sure that the **Tools** > **Compatibility View** option is not selected.

3 Navigate to **Tools** > **Internet Options** > **Security tab** > **Custom Level**, then scroll down to the **Downloads** section and select **Enable** under the **Automatic prompting for file downloads** option.

Change Guardian Agent for Windows Installation Using Agent Manager Fails

Issue: Change Guardian Agent for Windows installation using Change Guardian Agent Manager (CG AM) fails and displays the following error in failed task logs:

```
protocol negotiation failed...
```

This error might occur due to following reasons:

- SMB1 protocol is disabled on Change Guardian Agent for Windows.
- Change Guardian server is installed on SLES 11 SP4 or RHEL 6.7 platforms which supports SMBv1 only.

Workaround: Install Change Guardian Agent for Windows manually. For more information see “Manual Installation” on page 34.

Asset Monitoring Failure Reports are not Captured for All Event Types

Issue: The Asset monitoring failure reports are not captured for all event types such as audit failures, registry failures or system failures.

Workaround: To view the failure reports you must apply the policy where auditing mechanism of the specific event mentioned in the policy has failed.

Azure AD Monitoring Events are not Captured for All Event and Attribute Types

Issue: When you upgrade Change Guardian 5.0 to Change Guardian 5.1 or later, Change Guardian server is unable to fetch events for the newly added events and attributes. The events are not captured if you have selected “All Events” or “All Attributes” when you created the policy using Change Guardian 5.0.

Workaround: Perform the following procedure to overcome this issue:

1. . In the left pane of the Policy Editor window, select Azure Active Directory > Azure Active directory Policies.
2. Expand the Azure Active directory Policies and select the policy where you are monitoring “All Events” or “All Attributes”.
3. Click Edit and modify the description.
4. Click Submit.
5. Enable the policy revision.

Manual Configuration Required to use Registry Browser

Issue: To enable the Registry Browser in Change Guardian, you must set the `repositoryEnabled` flag (under `HKLM\Software\Wow6432Node\NetIQ\ChangeGuardianAgent\repositoryEnabled`) to `1`, and then restart the agent.

Workaround: Manually set the flag to `1`, when you use the Registry Browser, to avoid the error *Could not connect to Windows Data Source*. `(Bug 945225)`

Restarting the Change Guarding server with FIPS Mode Enabled Logs an Exception

Issue: If the Change Guardian server is FIPS-mode enabled and the server is restarted, the server logs an error message: "An unexpected exception occurred while decrypting data failed. Root cause: CKR_ENCRYPTED_DATA_INVALID (sun.security.pkcs11.wrapper.PKCS11Exception) java.security.ProviderException: doFinal() failed" (Bug 1129167)

Workaround: You can ignore the exception.

Change the Agent Package Version

Issue: You need to roll back to an older package of the agent package, but the Agent Manager does not allow you to change the agent package version. (Bug 1155538)

Workaround: You can enable a new package, and disable the previous package by using the following file `/opt/netiq/ams/ams/repository/packageActiveStatus.new.example`.

Installing Change Guardian Agent for Windows Fails with SMB Protocol Mismatch

Issue: Change Guardian Agent for Windows installation fails displaying the following error message in failed task logs: `Protocol negotiation failed...`. The error might occur due to the following reasons:

- SMB1 protocol is disabled on Change Guardian Agent for Windows.
- Change Guardian server is installed on a Linux version that does not support SMB Version 2 (such as SLES 11.x or RHEL 6.x that has kernel version 2.6.x or lower), but only supports SMB Version 1. `(Bug 1155405)`

Workaround: Upgrade the operating system, on which Change Guardian server is running, to a version that supports SMB Version 2.

Alternatively, you can manually install the latest version of Change Guardian Agent for Windows. For more information, see Installing Change Guardian Agent for Windows.

Change Guardian Web Console is Blank if the License Has Expired

Issue: If your Change Guardian license expires, the web console displays a blank page. `(Bug 949208)`

Workaround: Add the license through the command line by using the `softwarekey.sh` script. For more information, see *Adding a License Key* in the *Change Guardian User Guide*.

Unable to Browse File Locations And Active Directories Using Policy Editor File Browser

Issue: Following are the conditions:

- Unable to browse to file locations within a policy.
- Unable browse active directory from within a policy. (Bug 995355)

Workaround: To enable LDAP browsing in policy editor, perform the steps mentioned in NetIQ Knowledgebase Article 7017291.

Change Guardian Server Not Receiving Dell EMC Events

Issue: Change Guardian does not receive Dell EMC events if the CEPA server is not running. Accessing the CEPA from a browser shows that the site cannot be reached.

Workaround: Start the CEPA server

To start the server:

1. Open `services.mcs` and run the `EMC CAVA` service.
2. In the Dell EMC web-console, check if the CEPA IP is provided in the following format: `http://1.1.1.1:12228/cee`