Change Guardian™ 6.2

Installation and Administration Guide

May 2022

Legal Notice

Contents

13 Backing Up and Restoring Data 197

14 Upgrading Change Guardian Server 205

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:

Online Help

Provides information about the tasks that can be performed using the Change Guardian web console.

Release Notes

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

System Requirements

Provides the list of hardware and software requirements, and the supported applications.

1 Introduction

Change Guardian monitors critical files, systems, and applications in real-time to detect unauthorized activities of privileged users, helping you significantly reduce organizational risk to critical assets.

Change Guardian 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 13
- “How Change Guardian Works” on page 14

What is Change Guardian?

Change Guardian provides security intelligence to rapidly identify and respond to unauthorized activities of privileged users that indicate a security breach or compliance gaps. Change Guardian helps security teams to detect and respond to potential threats in real-time. Change Guardian achieves this 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 changes to critical files, platforms and systems to help prevent security breaches and ensure policy compliance.
- **Real-time change alerting**: Provides immediate visibility to unauthorized changes that could lead to a security breach, and enables a quick response to threats.
- **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**
- **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 the ability of SIEM solutions to detect and respond to security incidents by providing information about who did what, when, where, and how, along with providing before and after values. With this comprehensive security intelligence, you can mitigate the impact of an attack before severe damage or compliance gaps can occur.

Change Guardian monitors the following endpoints or assets: Windows Active Directory, Group Policy, Windows, Microsoft Azure Active Directory, AWS (Identity), Office 365, Dell EMC, Microsoft Exchange, NetApp, UNIX, and Linux.

How Change Guardian Works

There are innumerable activities that take place on an asset, and their corresponding events are logged in by the operating system. However, all events do not require attention or pose a threat to the organization. A policy defines filters, based on which Change Guardian collects events. A policy definition contains information about the type of events to collect, the users who are allowed to make the change, event severity, and so on. Change Guardian collects the events details such as who, what, when, and where. You can configure emails or alerts to receive notifications about the desired events.

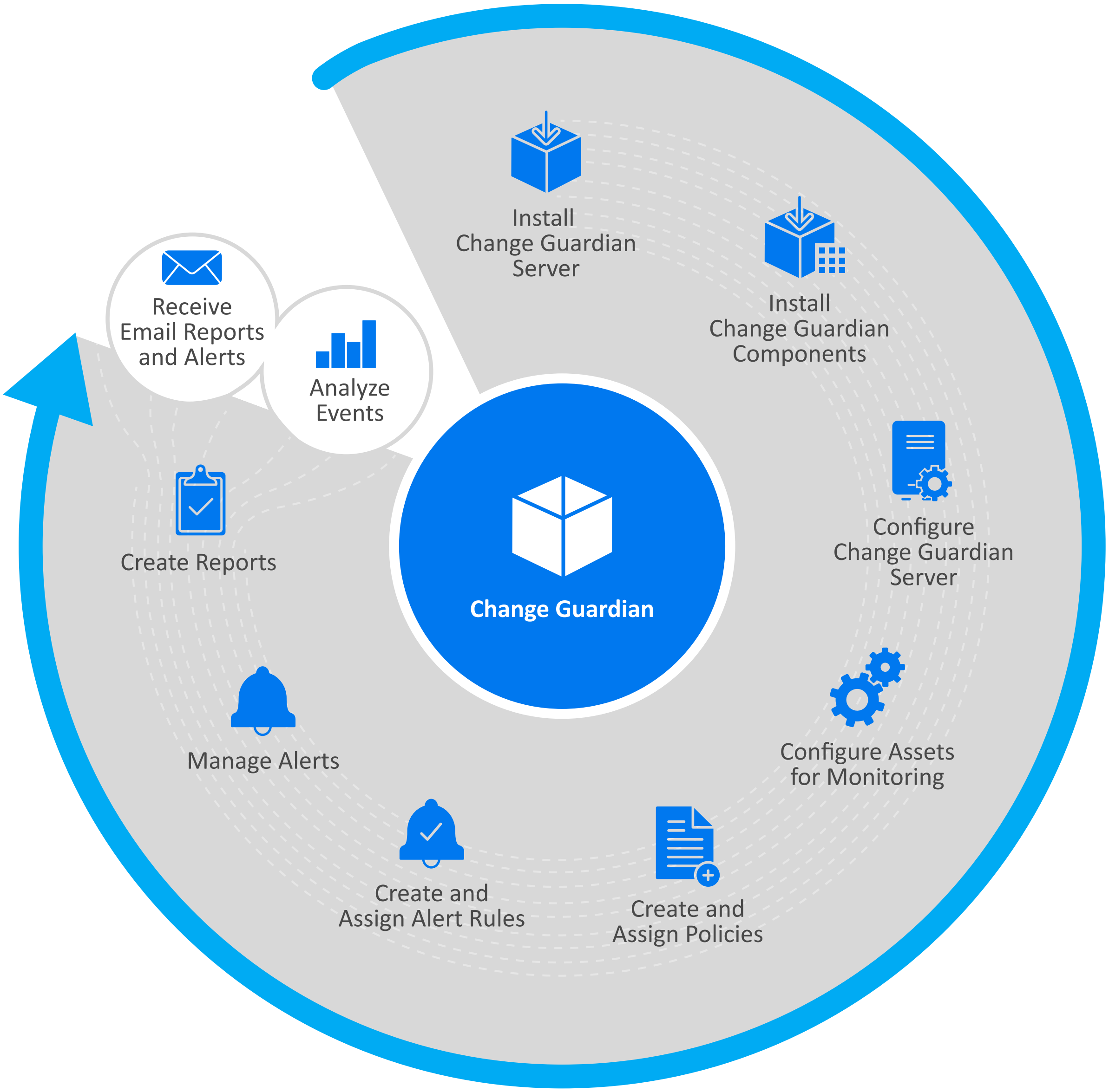
You can forward Change Guardian events to other software for further analysis and long term retention. You can forward events to another Change Guardian server, Sentinel server, Splunk Enterprise Security, or Micro Focus Security ArcSight Logger.

This section provides the following information:

- “Change Guardian Workflow” on page 14
- “Change Guardian Architecture” on page 16
- “Top User Scenarios” on page 17

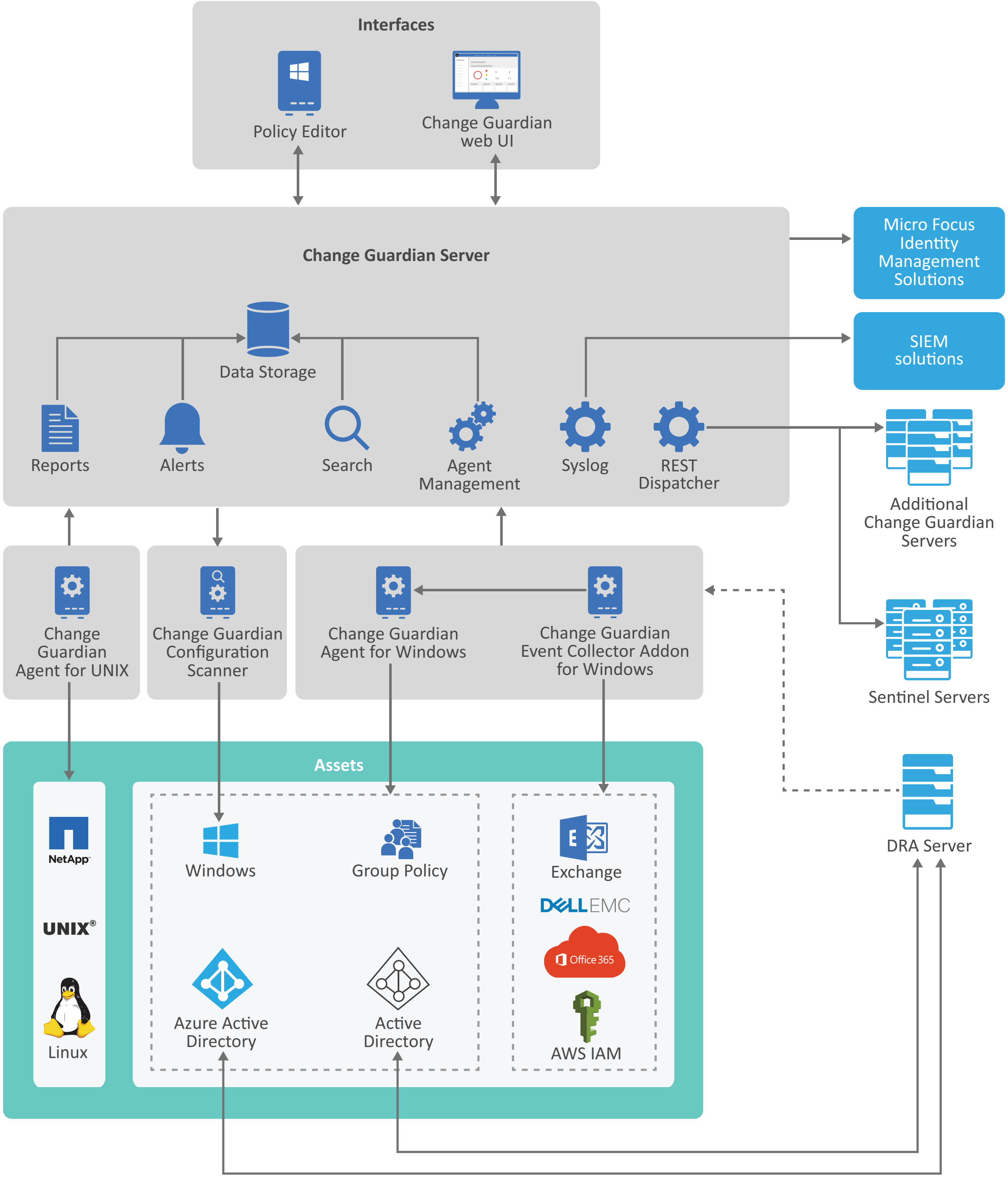
Change Guardian Workflow

The following diagram illustrates how Change Guardian interacts with different components:


Install
Change Guardian
Server
Install
Change Guardian
Components
Configure
Change Guardian
Server
Configure Assets
for Monitoring
Create and
Assign Policies
Create and
Assign Alert Rules
Manage Alerts
Create Reports
Analyze
Events
Receive
Email Reports
and Alerts
Change Guardian

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.

Components in the Diagram	Description
Change Guardian Agents	Windows or UNIX based software that collects event data from the assets and forwards them to the Change Guardian server.
Change Guardian Event Collector Addon for Windows Agent	Collects event data in the Common Event Format (CEF) from Dell EMC, Microsoft Exchange, AWS Identity and Access Management and Office 365. The Change Guardian Agent for Windows reads the event details in the CEF.
Change Guardian Server	A Linux-based computer that receives and stores the event data. The server also stores the policies that you create. You can also search for events, and create alerts and reports.
Agent Management	A central location where you can manage agents. You can deploy and manage your agents directly on the agent host machine, or remotely install agents using Agent Manager.
Policy Editor	A Windows-based console in which you can configure and manage policies, create and assign alert rules, configure event destinations, configure emails, and schedule monitoring.
Change Guardian Configuration Scanner	A Windows based component that collects configuration data of endpoints in an Active Directory environment.
Change Guardian Web UI	Interfaces to dashboards and management consoles where you can view event details and agent status, view and triage alerts, create event routing rules and alert routing rule, manage users, and so on.

Top User Scenarios

- “Monitoring a Privileged User Account” on page 17
- “Monitoring Changes to File Integrity” on page 18
- “Adhering to a Standard Benchmark” on page 18

Monitoring a Privileged User Account

Problem Statement: Adam Mandari is the Change Guardian administrator. His organization is required to adhere to the CIS policy “Audit Account Lockout is set to include Failure” for Microsoft Windows Server 2016. The policy mandates that multiple failed login attempts should be monitored. The Head of Security investigates such incidents for any breach of security.

Resolution: Adam has to monitor the user account ‘Payroll’ and monitor multiple failed logins associated with that account. Adam wants to configure an alert that notifies him when five unsuccessful login attempts made using ‘Payroll’ account.

Adam creates an Active Directory policy for Users Accounts `payroll_login_activity` with the following definition:

```
Monitors users accounts matching these user IDs Payroll
include only user account logged in events
include only failed events
```

Adam creates an alert rule specifying that an alert `alert_user_activity` should be generated when five events within 30 minutes are generated against the `payroll_login_activity` policy. He also configures an email server to be able to receive emails about the user account logged events.

Adam logs in to the Threat Response Dashboard to check the real-time alerts. When he receives the alert `alert_user_activity` in the dashboard, he finds the details of the `user account logged in` event. The event provides information about the machine from where the event occurred, the time at which the event occurred. Using the Threat Response Dashboard, he can decide to set a custom priority and assign it to another administrator to investigate the event.

To monitor this event regularly, Adam uses the Event Dashboard and looks for the `user account logged in` event. Every week, Adam exports the event details as a report and shares with the Head of Security.

Monitoring Changes to File Integrity

Problem Statement: Adam Mandari must ensure that his organization adheres the CIS policy “Audit Policy Change is set to include Success” for Microsoft Windows Server 2016. The policy mandates that critical Human Resource files are modified within the domain of the organization.

Resolution: Adam wants to use the real-time change monitoring feature in Change Guardian. Being the Change Guardian administrator, he creates a Change Guardian for Windows policy to monitor the changes to the specific folder, having the following definition:

```
Monitors changes to contents in files in c:\payroll whose patterns match *
include only file content difference events
```

When an attempt is made to modify any files in the `C:\payroll` directory, Change Guardian Agent for Windows collects the “File integrity was changed” event from the Windows machine and sends it to the Change Guardian server. The event contains the name of the event, the Windows machine details, the user who triggered the event, the time at which the write action was performed, and the old and the changed content. He logs in to the web console and uses the Event Dashboard to view the event. Adam configures an alert that notifies him whenever “File integrity was changed” event is generated. To analyze the real-time alerts he uses the Threat Response Dashboard.

Adhering to a Standard Benchmark

Problem Statement: Adam Mandari is the Change Guardian administrator and he would like to ensure that all assets are running and they are constantly monitored by Change Guardian policies. He has to ensure that the company adheres to the CIS for Microsoft Windows Server 2016.

Resolution: Before creating a Change Guardian policy to monitor the computers, Adam ensures that the computers are communicating with the Change Guardian server and that there are no auditing related issues. Adam logs in to the web console and uses the Agent Health Dashboard to identify the status of Change Guardian agents. He reviews the diagnostic information of the agents in the warning state and identifies the auditing related issue. After resolving the issues, he logs in back to the Agent Health Dashboard to view the updated status. When all Change Guardian agents are online, Adam uses Policy Editor to create policies in Change Guardian that ensure that the company adheres to CIS standards. He assigns the policies to agents to enable continuous monitoring.

2 Preparing for Installation and Upgrade

This section provides information about planning Change Guardian installation and upgrade.

- "Implementation Checklist" on page 21
- "Installation and Upgrade Options" on page 22
- "Security Considerations" on page 22
- "Understanding Application Licensing" on page 23
- "Understanding Ports Used" on page 23

Implementation Checklist

Use the following checklist before you begin installing or upgrading Change Guardian server:

	Task	See
□	Review the hardware and software requirements, and the supported applications	Change Guardian System Requirements
□	Determine the method to install or upgrade the Change Guardian server	Install and Upgrade Options
□	Determine whether you want to **install** or **upgrade** the Change Guardian server	Install the Change Guardian server Upgrade the Change Guardian server
□	**Install** or **upgrade** the Change Guardian components	Install the Change Guardian components Upgrade the Change Guardian components
□	Configure Change Guardian after the **installation** or **upgrade**	Configure the Change Guardian server after installation Complete the post upgrade configurations
□	Configure Policies	Configure Policies
□	Manage Events	Manage Events
□	Configure Alerts	Configure Alerts

Installation and Upgrade Options

Use this section to determine the option to installation or upgrade the Change Guardian server.

Traditional method

The traditional installation or upgrade provides the following:

- The flexibility to select the operating system vendor of your choice
- The flexibility to set firewall yourself
- More customization options for product configuration during installation

Appliance method

The appliance installation or upgrade provides the following:

- A ready-to-run Change Guardian software appliance with inbuilt SLES operating system
- 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

The following sections provide information about secured installations:

- "Traditional Installation" on page 22
- "Appliance Installation" on page 23

Traditional Installation

- Close all unnecessary ports. To review the list of ports, see "Understanding Ports Used" on page 23.
- 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.

Understanding Application Licensing

You require an application license to enable Change Guardian to monitor the specific application. For information about the number of licenses required for each application, see the following table:

Application Name	License Count
Windows	Number of monitored Windows servers or workstations
UNIX	Number of monitored UNIX, Linux, or UNIX-derivative servers or workstations
Active Directory and Group Policy	Number of enabled active users in Active Directory
	Number of enabled active users in Group Policy
NetApp	Number of monitored NetApp instances
Azure AD	Number of enabled active users in Azure Active Directory
Microsoft Exchange	Number of active Exchange users
EMC	Number of monitored Dell EMC instances
AWS IAM	Number of active AWS identities
O365	Number of active users in Exchange Online

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.
Change Guardian Server	TCP 8077	Outbound	Required	Allows the Change Guardian Server to connect to the Change Guardian Scanner service.
	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	Used if secondary storage is configured to CIFS.

Component	Ports	Direction	Required/ Optional	Description
	TCP/UDP 111 and TCP/UDP 2049	Outbound	Optional	Used if secondary storage is configured to NFS.
	UDP 514 or TCP 1468	Outbound	Optional	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 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 Correlation Engines.
	TCP 9443	Inbound	Required	Used by the Change Guardian Appliance Management Console.
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.

Component	Ports	Direction	Required/ Optional	Description
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.
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.
Change Guardian Scanner Service	TCP 8077	Inbound	Required	Allows the Change Guardian Server to connect to the Change Guardian Scanner service.

3 Installing Change Guardian Server

This chapter guides you through installing the Change Guardian server.

- "Traditional Change Guardian Server Installation" on page 27
- "Change Guardian Server Appliance Installation" on page 33
- "Verifying the Installation" on page 37

Traditional Change Guardian Server Installation

This section provides the following information:

- "Prerequisites" on page 27
- "Installing the Change Guardian Server" on page 28

Prerequisites

Ensure that your system meets the following:

- Review the Change Guardian Release Notes to understand new features and known issues.
- Review the System Requirements to understand the memory and CPU requirements.
- Change Guardian is not supported if the operating system is in FIPS mode. Therefore, ensure that the operating system is not in FIPS mode.
- NTP synchronized your computer time with the network time.
- 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:
  - zip
  - unzip
  - 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
- insserv-compat (applicable on SLES server)
- pam-modules (available only when you install Legacy-Module on SLES server 15.x)
- Packages applicable for installation on RHEL and SLES 15 SP2 command-line interface:
  - libX11
  - libXext
  - libXi
  - libXrender
  - libXtst
  - libwbclient
  - cups-libs
  - libtdb
  - libldb
  - gnutls
- zlib (up to SLES 12.x and RHEL 7.x, 8.x)
- python-libs (up to SLES 12.x and RHEL 7.x)
- netstat (up to SLES 12.x and RHEL 7.x) or ss (for SLES 15 and later)

NOTE: If there was a previous installation of Change Guardian, ensure that there are no files or system settings remaining from a previous installation.

Installing the Change Guardian Server

You can use either of the following methods to install Change Guardian server:

- "Performing an Interactive Installation" on page 29
- "Performing a Silent Installation" on page 33

NOTE: 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, consider using static IP addresses in your Change Guardian deployment.

Performing an Interactive Installation

This section provides information about standard and custom installation.

- "Standard Installation" on page 29
- "Custom Installation" on page 31

Standard Installation

Use the following steps to perform a standard installation:

To install the Change Guardian server:

1. Download the Change Guardian installation file from the Downloads website.
2. On the command line, log in as the `root` user and type the following command to extract the installation file:

   ```
   tar zxvf change_guardian-<version>.tgz
   ```
3. Run the Change Guardian server installation program as `root` 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-changeguardian.sh -r <response_filename>`
4. (Conditional) If NTP could not synchronize your computer time with the network time, make the required changes to the computer.
5. (Conditional) If your system does not meet the recommended disk space, make the required changes to the computer.

   NOTE: Ensure that the disk has the recommended space for Change Guardian installation files. Allocate recommended space in `/`, `/var/opt`, and `/opt`.
6. Specify the language as English, then press Enter. The end user license agreement is displayed in the selected language.
7. Press the space bar to read the license agreement. You must scroll through the entire agreement before you can accept it.
8. When prompted, select the standard configuration.
9. Create an admin account password for global system administration.

NOTE: Until Change Guardian 6.2 version, while setting the admin password, only the following non-alphanumeric characters are allowed:` ! @ $ ^ _ { } [ ] \ : " , . / ?. From version 6.2.1.0, all non-alphanumeric characters are allowed to be used to set the password.

10 Create a password for the `cgadmin` user.

Use this account to log in to Policy Editor. `cgadmin` has administrative rights to monitor configurations.

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

11 If you want to email reports, 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. Change Guardian server should be able to resolve the hostname.
- **SMTP Port:** The remote SMTP port, where the default number is 25. Use port 587 for a secure connection.
- **From:** The return email address.
- **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: If you later decide to email reports and events, you must use the `configure.sh` script to update this configuration. For more information, see "Configuring Email Server to Receive Email Alerts" on page 73.

11a (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 trust-store. To import the self-signed certificate or CA certificate, complete the following steps:

11a1 Download the certificate to the server.

11a2 To store the certificate in `activemqkeystore`, run the following command on the server:

```
/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
```

11a3 Restart the server:

```
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 starts all services before you log in to the server.

To install the Change Guardian components, see "Installing Change Guardian Components" on page 39.

Custom Installation

To install the Change Guardian server:

1 Download the Change Guardian installation file from the Downloads website.

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

```
tar zxvf change_guardian-<version>.tgz
```

3 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. Ensure that you allocate the recommended disk space in / and /home.

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-changeguardian.sh --location=<custom_CG_directory_path> -r <response_filename>
```

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

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

6 When prompted, select custom configuration, and provide 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

---

NOTE: Until Change Guardian 6.2 version, while setting the admin password, only the following non-alphanumeric characters are allowed:`` ` ! @ $ ^ _ { } [ ] \ : " , . / ? ``. From version 6.2.1.0, all non-alphanumeric characters are allowed to be used to set the password.

Assign dbauser account password: Account for PostgreSQL database maintenance

Assign appuser account password: Account for connections with PostgreSQL database at runtime

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

---

NOTE: Changing the default database service port 5432 might cause Change Guardian to behave inconsistently.

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

---

NOTE: 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 77

---

7 Create a password for the `cgadmin` user.

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. Change Guardian server should be able to resolve the hostname.
- **SMTP Port:** The remote SMTP port, where the default number is 25. Use port 587 for a secure connection.
- **From:** The return email address.
- **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: If you later decide to email reports and events, you must use the `configure.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 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 on the server:

```
/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 starts all services start before you log in to the server.

To install the Change Guardian components, see “Installing Change Guardian Components” on page 39.

Performing a Silent Installation

The silent or unattended installation is useful if you need to install more than one Change Guardian instance 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 Downloads website.
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 change_guardian-<version>
   ```

4. To install in silent mode, specify the following command:

   ```
   ./install-changeguardian -u <response_filename>
   ```

   The installation proceeds with the values stored in the response file.

   After the installation finishes, you can log in to the server. To install the Change Guardian components, see "Installing Change Guardian Components" on page 39.

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

Change Guardian 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.

NOTE: 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, consider using static IP addresses in your Change Guardian deployment.

Prerequisite: Ensure the following:

- the machine meets the hardware requirements. For hardware information, see the System Requirements page.
- NTP synchronized your computer time with the network time.

To install:

1. Download the base appliance image to a local server from the Downloads website.

   The OVF file name is change_guardian_appliance_<*version*>.ovf.tar.gz

   The ISO file name is change_guardian_appliance_<*version*>.iso

   The VHD file name is change_guardian_appliance_<*version*>.zip

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, such as WinRar:

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

   ```
   tar -zxvf <filename>
   ```

   2b Log in to the vSphere client and deploy the OVF template. For more information, see the VMware documentation.

3. (Conditional) If you are installing directly to hardware, use the ISO image to complete the following steps:

   3a Burn the ISO file to a DVD or mount the image.

   NOTE: Change Guardian does not support mounting the ISO image from a network share.

   3b Start or reboot your computer and check the BIOS configuration of your machine. The 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. (Conditional) If you are using Hyper-V, see "Configuring Microsoft Hyper-V Appliance" on page 35.

5. Power on the appliance server.

6. Select the language and keyboard layout.

7. Read and accept the SUSE End User License Agreement.

8. Read and accept the Change Guardian End User License Agreement.

9. On the Change Guardian Appliance Passwords and Time Zone screen, specify the following:

   - Change Guardian root and vaadmin passwords
   - NTP server details
   - Region and time zone of the virtual machine

10. On the Change Guardian Server Configuration screen, specify the following:

    - Global admin password

    NOTE: Until Change Guardian 6.2 version, while setting the admin password, only the following non-alphanumeric characters are allowed:` ! @ $ ^ _ { } [ ] \ : " , . / ?. From version 6.2.1.0, all non-alphanumeric characters are allowed to be used to set the password.

    - cgadmin user password
    - Deselect Use IP Address for event routing

    Change Guardian server should be able to resolve the hostname.

- (Optional) If you want to email reports, configure the default email server:
    - Specify the full name, including the domain name, of the email server as the `SMTP server hostname`. This is the server from which you want to send email notifications.

      Change Guardian server should be able to resolve the hostname.
    - Specify the `SMTP server port`. The default port is 25. Use port 587 for a secure connection.
    - Specify the return address in `From Address`.
    - Specify the SMTP username and password to connect to the SMTP server.

11. On the Change Guardian Appliance Network Settings, specify the hostname and the mechanism to assign the IP address of the virtual machine.

    Optionally, you can configure the network proxy.
12. The script checks whether your system meets the minimum requirement of CPU core and memory. Specify `Next` to continue or `Abort` to stop the installation.
13. (Conditional) If javos service does not run after completing this step, reconfigure Change Guardian by using configure.sh.

This completes the Change Guardian server installation. To install the Change Guardian components, see "Installing Change Guardian Components" on page 39.

NOTE: If the server time appears out of sync immediately after the installation, restart NTP:

```
service ntp stop

service ntp start
```

Configuring Microsoft Hyper-V Appliance

You can install Change Guardian appliance on Hyper-V 2016 and Hyper-V 2019.

NOTE: Change Guardian documentation provides the third-party configuration steps for ease of use. For more information about the third-party products or for any issues with the configuration, see their documentation.

To configure:

1. Log in to the host server either locally or from a remote workstation.

   You can use Windows Remote Desktop to log in to the host server from a remote workstation.
2. Create a new directory in the location where you want the virtual machine to reside.

   As a best practice, use the same name for the directory and the appliance virtual appliance.
3. Download the software to the new directory, and extract the Change Guardian appliance `.zip` file.
4. Open Hyper-V Manager.
5. On the left pane, right-click the host name and click **New > Virtual Machine**.

   This is the host where you want to create the new virtual machine.

6. Follow the wizard and provide the following information:
   - Specify the name of the virtual machine
   - In **Specify Generation** page specify the generation as Generation 1
   - In **Assign Memory** page, specify the amount of memory (in MB) to allocate to the virtual machine. For details, see the Change Guardian System Requirements page.
   - In **Configure Networking** page, specify the connection mechanism.
   - In **Connect Virtual Hard Disk** page, select **Use an existing virtual hard disk,** and browse to the `.vhd` file.
7. Right-click on the newly created virtual machine, and click **Settings > Processor** and specify the number of virtual processors.
8. Right-click on the virtual machine and click **Connect** to open it.
9. Right-click on the virtual machine and click **Start**.
10. Continue to step 6 to complete installing the Change Guardian appliance.

NOTE: Change Guardian Hyper-V appliance deploys a virtual machine with 100 GB disk. To expand the disk space, check the recommended disk space in the System Requirements page. You must expand the disk immediately after installing the Change Guardian Hyper-V appliance. To expand the `/var/opt` partition, see "Expanding Disk Space in Hyper-V Virtual Machine" on page 247.

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 the Change Guardian Appliance Management Console" on page 36
- "Register Using Commands" on page 37

Register Using the Change Guardian Appliance Management Console

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.
7. To view the registration status of the appliance, click **Register**.

NOTE: When you apply appliance patches on Change Guardian appliance using Management console, you will see a conflict for 2 OS patches (`SUSE-SU-2021:3649, SUSE-SU-2022:0323`). Switch to command-line method to proceed with the upgrade. For more information, refer from step 6 in Applying Updates Using Zypper.

Register Using Commands

Use the following steps to register the appliance using the command line:

1. Log in to the Change Guardian Appliance Console as `root`: `https://IP_Address_Change_Guardian_server:9443.`
2. Clean existing registrations for SLES (11 and 12) based clients:

   ```
   suse_register -E
   ```
3. Register the server for SLES (11 and 12) based clients:

   ```
   suse_register -a regcode-change-guardian="<registration_code>" -a
   email="<email_ID>"
   ```
4. Verify whether updates are available.

Verifying the Installation

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

- Ensure the server is up: `netstat -an | grep LISTEN | grep <port_number>`

  The possible *port_number* are 8443, 9443, 8094, or 8082. For example, running the command with ports 8443 and 9443 might provide the following output:

  ```
  tcp6       0      0 :::8443    :::*    LISTEN
  tcp        0      0 :::9443    :::*    LISTEN
  ```
- Ensure the server ports such as 8443, 8094, 8082 and 9443 are open:
  - On SLES, run the following command in the server:

    ```
    iptables -I INPUT -p tcp --dport <port_number> -j ACCEPT
    iptables-save
    ```
  - On RHEL, run the following command in 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 23.
- Access the Change Guardian dashboard:

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

4 Installing Change Guardian Components

After installing the Change Guardian server, you must install a combination of Change Guardian components. Following are Change Guardian components:

Policy Editor: Allows you to configure Change Guardian policies.

Change Guardian Agent for Windows: Collects event data for the supported assets, such as Windows, Windows Active Directory, and Azure Active Directory.

Change Guardian Event Collector Addon for Windows Agent: Collects event data in Common Event Format (CEF) from assets, such as Dell EMC, Microsoft Exchange, and Office 365, which is used by Change Guardian Agent for Windows.

Change Guardian Agent for UNIX: Collects event data for Linux, UNIX, and NetApp.

Change Guardian Configuration Scanner: Collects configuration data of endpoints in an Active Directory environment.

For information about requirements and recommendations, see the System Requirements page.

Install the components using Agent Manager. To open Agent Manager, open the Change Guardian web console and click **AGENTS**.

This chapter provides the following information:

Installing Policy Editor

To install Policy Editor:

1. In Agent Manger, click **All Assets > Manage Installation > Download Package**.
2. Download the available version of Policy Editor.
3. Copy the `ChangeGuardianPolicyEditor.zip` file to the computer where you want to install Policy Editor and extract the files.

   The package includes `NetIQCGPolicyEditorInstaller.exe` and `NetIQCGPolicyEditorInstaller.exe.config`. Both files must be in the same directory.
4. Install Policy Editor as an administrator.

Verifying the Installation

To verify:

- Ensure that Policy Editor is available in the list of installed programs in Windows Control Panel
- Launch Policy Editor and log in with an account in the local administrators group

  When Policy Editor starts, it connects to the Policy Repository with an account that is a member of the administrator or Change Guardian administrator role. The Policy Repository runs on the Change Guardian server.

Installing Change Guardian Agent for Windows

- "Interactive Installation" on page 40
- "Verifying the Installation" on page 41

For troubleshooting information about Change Guardian Agent for Windows, see "Issues on Change Guardian Agent for Windows" on page 232.

Interactive Installation

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

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

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

Remote Installation

Remote installation using Agent Manager provides a convenient and uniform method for installing one or more Change Guardian Agent for Windows. When you use Agent Manager to install, Agent Manager communicates with the agent through the Agent Management service.

Prerequisite: Using Agent Manager, you must first add the assets where you want to install agents. You can either import assets from Active Directory or from a text file, or add assets manually. For more information, see "Adding Assets" on page 81.

To install Change Guardian Agent for Windows using Agent Manager:

1. In Agent Manager, select the asset where you want to deploy the agent. If you select multiple assets, they must use the same credentials.
2. Click **Manage Installation > Install Agents**.
3. For newly added assets, specify the `root` credentials and click **Next**.

   NOTE: Log in to the newly added asset as an administrator to the deploy agent. The account must be a local administrator or a domain account in the Local Administrators group.

4. Select the available version of the agent.

5 For agent configuration, select any one option: default agent configuration, customize the configuration, or add new.

6 Click **Start Installation.**

Manual Installation

Manual installation includes installing the agent certificates and artifacts, along with the agent.

- "Downloading the Agent Certificates and Artifacts" on page 41
- "Installing the Agent" on page 41

Downloading the Agent Certificates and Artifacts

Use Agent Manager to download and install agent artifacts and certificates on one or more hosts.

NOTE: You must install agent artifacts and certificates for each host separately.

To download:

1 In Agent Manager, click **All Assets > Manage Installation > Download**.

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

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

4 Copy and extract the `ChangeGuardianAgentCertificates_<hostname>.zip` file to the agent artifact directory, before installing the agents.

Installing the Agent

To install:

1 From Agent Manager, download the available version of Change Guardian Agent for Windows.

2 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.

3 Run the `NetIQCGAgentSilentInstaller.exe` file as an administrator.

Verifying the Installation

To verify:

- Ensure that Change Guardian Agent is available in the list of installed programs in Windows Control Panel

- Ensure that the service NetIQChangeGuardianAgent is running in Windows Services
- If you used Client Agent Manager to install, ensure that Client Agent Manager is available in the list of installed programs in Windows Control Panel. Also ensure that the service NetIQClientAgentManager is running in Windows Services

Installing Change Guardian Event Collector Add-on for Windows Agent

Change Guardian Event Collector Add-on for Windows Agent collects events in the common event format (CEF). Change Guardian supports events only in CEF.

Before installing the Change Guardian Event Collector Add-on for Windows Agent, set up the required connectors.

NOTE: Change Guardian documentation provides the configuration steps about third-party products AWS, Office 365, Dell EMC, and Exchange for ease of use. For more information about the third-party products or for any issues with the configuration, see their documentation.

- “Prerequisites for AWS” on page 42
- “Prerequisites for Office 365” on page 44
- “Prerequisites for Dell EMC” on page 45
- “Prerequisites for Exchange” on page 46
- “Installing Change Guardian Event Collector Addon for Windows Agent” on page 49

Prerequisites for AWS

This section provides the following information:

- “Setting the AWS Account” on page 42
- “Configuring CloudTrail” on page 43
- “Creating and Subscribing an Amazon Simple Queue Service (SQS)” on page 43
- “Important Parameters” on page 44

For information about AWS concepts, see *AWS Documentation* (https://docs.aws.amazon.com/).

NOTE: Ensure that you have the required permission to complete these tasks. Check with your network or system administrator for assistance.

Setting the AWS Account

If you are using Elastic Compute Cloud (EC2) role-base credentials, then you must use an IAM role with `AmazonS3ReadOnlyAccess` and `AmazonSQSFullAccess` policies. If you are using access key or secret key as credentials, complete the following steps:

To setup:

1. Create an Amazon Web Services account.
2. Log in to the **AWS Management Console** and open **IAM**.
3. From **Dashboard**, click **Access Management > Groups > Create New Group.**
4. Specify **Group Name** and attach the policies **AmazonS3ReadOnlyAccess** and **AmazonSQSFullAccess** to the group.

   The group requires necessary permissions to access the CloudTrail logs through APIs.
5. To add new user to the group, select **Users > Add Users**.
6. Specify the user details.
7. Ensure that you download the credentials as `.csv` file.

   NOTE: The file contains the **Access Key ID** and **Secret Access Key** that you have to use when installing the connector.
8. Click **Groups >** ***group_name*** **> Group Action > Add Users to Group**.
9. Select the users to add to the group and click **Add Users**.
10. To view or create an Access key ID, open user summary and click **Security Credentials > Create Access key**.

Configuring CloudTrail

Create a new Amazon Simple Storage Service (S3) bucket and a new Amazon Simple Notification Service (SNS) topic.

To configure CloudTrail:

1. From the AWS Management Console, open **CloudTrail**.
2. Click **Create trail**.
3. Specify **Trail name**.
4. Select **Create new S3 bucket** and specify **Trail log bucket and folder**.
5. Select **SNS notification delivery**.
6. Select **Send SNS notification for every log file delivery**.
7. Specify a new SNS Topic.

Make a note of the **AWS S3 Region** name available at the browser address box of the SQS page.

Creating and Subscribing an Amazon Simple Queue Service (SQS)

To create an SQS:

1. In the AWS Management Console, open **Simple Queue Service**.
2. Click **Create New Queue** and specify the details.
3. Select the new queue.

4 Under **Queue Actions**, select **Subscribe Queue to SNS Topic**.

5 From **Choose a Topic**, select the new topic and click **Subscribe**.

Important Parameters

You should have the following parameters after setting up AWS. Use these parameters to install Change Guardian Event Collector Addon for Change Guardian:

Parameter	Description
Proxy Host	(Optional) The proxy configuration settings
Proxy Port	
Proxy User Name	
Proxy Password	
AWS SQS URL	The SQS URL from which you want to pull the CloudTrail notification
AWS Access Key	The credentials for the IAM user
AWS Secret Key	
AWS SQS Region	The locations of AWS data centers
AWS S3 Region	
AWS SQS Visibility Timeout	The time during which Amazon SQS prevents other consuming components from receiving and processing that message
AWS SQS Max Received Count	The maximum number of attempts to receive an SQS message

Prerequisites for Office 365

Register the connector in Azure AD and configure it with appropriate permissions. Ensure that you have enabled and configured Office 365 subscription account. Also, ensure that the subscription is associated with an Azure AD Tenant Domain account.

NOTE: Ensure that you have the required permission to complete these tasks. Check with your network or system administrator for assistance

Registering the Application in Azure AD

To register:

1 Log in to the Azure Management portal using the credentials of your Microsoft tenant that has the subscription to Office 365 you wish to use.

2 Click **Azure Active Directory**.

3 Under **Manage**, click **App registrations > New registration**.

4. Specify a logical name, supported account types, redirect URI (optional), and then click **Register**.

   Make a note of the **Application (Client) ID**, which is the **Client ID**.

5. Under **Manage > Certificates and secrets > New client secret**, specify the client secret details and click **Add**.

   Make a note of the **Client secret value (ID)**, which is the **Client Secret**.

6. Click **API permissions > Add a permission > Office 365 Management APIs > Delegated permissions and Application Permissions**.
7. Select **ActivityFeed.Read**, **ActivityFeed.ReadDlp** and **ServiceHealth.Read** and click **Add permissions**.
8. On the API permissions page, click **Grant admin consent for <*organization name*>**.

Important Parameters

You should have the following parameters after setting up Office 365. Use these parameters to install Change Guardian Event Collector Addon for Change Guardian:

Parameter	**Description**
Azure Tenant Domain	The domain name of the Office 365 Azure tenant
Client ID	The Client ID of the registered application in Azure Active Directory
Client Secret	The Client Secret of the application registered in Azure Active Directory
Proxy Host	(Optional) Proxy configuration setting
Proxy Port	
Proxy User Name	
Proxy Password	

Prerequisites for Dell EMC

NOTE: Ensure that you have the required permission to complete these tasks. Check with your network or system administrator for assistance

Installing Common Event Enabler

To install Common Event Enabler (CEE):

1. Log into the machine with the account that has administrator privilege.
2. Ensure that .NET Framework 3 is enabled.
3. Run the file `EMC_CEE_Pack` for either the 32-bit (WIN32) or the 64-bit (X64) version of the software.
4. Follow the prompts and complete the installation.

NOTE: Do not change the location of the temporary directory.

5 When installer prompts you to restart the server, Click **No**.

6 Open `services.mcs` and search for `EMC CAVA` in the services list.

7 Right click **Properties** and click **Log On > This Account > Browse > Advanced > Find Now**.

8 Select the administrator or the account with administrative privilege and set the password.

9 Restart the machine.

10 Access the CEPA server from a browser.

Use the same format that you provided in the Dell EMC web console, for example, `http://1.1.1.1:12228/cee`.

If the CEPA server is running, it displays the version of CEE.

To set up application access:

1 Open Windows registry and open **HKEY_LOCAL_MACHINE > SOFTWARE > EMC > CEE > CEPP > Audit > Configuration**.

2 Specify `ArcSightConnector` in **Endpoint**.

3 Specify 1 in **Enable**, and restart the machine.

Important Parameters

You should have the following parameters after setting up Dell EMC. Use these parameters to install Change Guardian Event Collector Addon for Change Guardian:

Parameter	Description
Domain Name Domain Host Name Domain User Name Domain Password	The domain controller details to perform SID translation of users

Prerequisites for Exchange

The Exchange Management Shell is built on Windows PowerShell technology. With the Shell, you can manage every aspect of Exchange, including enabling new e-mail accounts, configuring SMTP connectors, storing database properties, storing transport agents, and more. The Shell can perform every task that can be performed by the Exchange Management Console and the Exchange Web interface, in addition to tasks that cannot be performed in those interfaces.

NOTE: Ensure that you have the required permission to complete these tasks. Check with your network or system administrator for assistance

This section provides the following information:

- "Enabling Mailbox Audit Logging" on page 47
- "Enabling Administrator Audit Logging" on page 47
- "Enabling Execution of Microsoft Exchange PowerShell Scripts" on page 48
- "Configuring Microsoft Exchange PowerShell" on page 48
- "Locating the Fully Qualified Domain Name" on page 48
- "Important Parameters" on page 48

Enabling Mailbox Audit Logging

To understand mailbox audit logging, see *Messaging policy and compliance permissions* in the Microsoft Exchange Documentation.

Use the Shell to specify Mailbox Audit Logging Settings, and specify logging settings for Administrator, Delegate, and Owner access.

1. Enable mailbox audit logging for Ben Smith's mailbox:

   ```
   Set-Mailbox -Identity "Ben Smith" -AuditEnabled $true
   ```

2. For detailed syntax and parameter information, see *Set-Mailbox* in the Microsoft Exchange Documentation.
3. Specify that the SendAs or `SendOnBehalf` actions performed by delegate users are logged for Ben Smith's mailbox:

   ```
   Set-Mailbox -Identity "Ben Smith" -AuditDelegate SendAs,SendOnBehalf -
   AuditEnabled $true
   ```

4. Specify that the `MessageBind` and `FolderBind` actions performed by administrators are logged for Ben Smith's mailbox:

   ```
   Set-Mailbox -Identity "Ben Smith" -AuditAdmin MessageBind,FolderBind -
   AuditEnabled $true
   ```

5. Specify that the HardDelete action performed by the mailbox owner will be logged for Ben Smith's mailbox.

   ```
    Set-Mailbox -Identity "Ben Smith" -AuditOwner HardDelete -AuditEnabled
   $true
   ```

Enabling Administrator Audit Logging

To understand administrator audit logging, see *Administrator audit logging in Exchange Server* and *Exchange and Shell Infrastructure Permissions* in the Microsoft Exchange Documentation.

Use the Shell to specify Administrator Logging Settings, and specify logging settings for Administrator, Delegate, and Owner access.

1. Enable administrator audit logging:

   ```
   Set-AdminAuditLogConfig -AdminAuditLogEnabled $True
   ```

2. Enable administrator audit logging for every cmdlet and every parameter in the organization, with the exception of Get Cmdlets:

```
Set-AdminAuditLogConfig -AdminAuditLogEnabled $true -
AdminAuditLogCmdlets * -AdminAuditLogParameters *
```

3. Enable administrator audit logging for specific Cmdlets run in the organization:

   ```
   Set-AdminAuditLogConfig –AdminAuditLogEnabled $true -
   AdminAuditLogCmdlets *Mailbox* -AdminAuditLogParameters *Address*
   ```

   Any parameter used on the specified Cmdlet is logged. Every time a specified cmdlet is run, a log entry is added to the audit log.

Enabling Execution of Microsoft Exchange PowerShell Scripts

Allow Microsoft Exchange PowerShell scripts to execute so that it can collect information about mailboxes and events from Microsoft Exchange.

To enable:

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**.

Configuring Microsoft Exchange PowerShell

You must configure Microsoft Exchange PowerShell services to run with a privilege to receive exchange audit log.

To allow the services to run 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.

Locating the Fully Qualified Domain Name

To allow Change Guardian Event Collector Addon for Windows Agent to retrieve events from the correct source, find the FQDN. Go to **System** in Windows Control Panel. Under Computer name, domain, and workgroup settings, and find the Full computer name.

Important Parameters

You should have the following parameters after setting up Exchange. Use these parameters to install Change Guardian Event Collector Addon for Change Guardian:

Parameter	Description
Server FQDN	The fully qualified domain name to the Exchange Server
Frequency	The frequency, in seconds, at which each mailbox audit log is retrieved
PowerShell Path	The location of the PowerShell application

Installing Change Guardian Event Collector Addon for Windows Agent

To install Change Guardian Event Collector Addon for Windows Agent:

1. In Agent Manager, click **Manage Installation > Download Package**.
2. Download Change Guardian Event Collector Addon for Windows Agent.
3. In the installer window, specify the local path in which you want to install Change Guardian Event Collector Addon for Windows Agent.
4. Select the connectors to configure.
5. Specify the location to store events in CEF.

   NOTE: Specify the same path in **CEF Data Output Path** in Agent Manger.

6. Specify the 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 exceeds the set value. If the EPS is low in AWS IAM, set the file rotation and file size values lower than the default.

7. Specify the parameters for the selected connectors.

If your connector is	Do this
Dell EMC	Specify the following: ◆ Domain name, hostname, user name, and password ◆ Enable SID Translation
Microsoft Exchange	Specify the following: ◆ Server FQDN ◆ Frequency Set any value between 1 and 600

If your connector is	Do this
AWS IAM	Specify the following: ◆ (Optional) Proxy details such as host, port, username, and password ◆ AWS Access Key ◆ AWS Secret Key ◆ AWS SQS URL ◆ AWS SQS Region ◆ AWS SQS Visibility Timeout ◆ AWS SQS Max Received Count ◆ AWS S3 Region
Office 365	Specify the following: ◆ Azure Tenant Domain ◆ Client ID ◆ Client Secret ◆ (Optional) Proxy server, port, username, and password

8 (Optional) Open Windows services, and restart the following services:

- **ArcSight Dell EMC Unity and VNXe Storage**
- **ArcSight Microsoft Exchange PowerShell**
- **Arcsight Microsoft Office 365**
- **Arcsight Amazon Web Services CloudTrail**

NOTE: After the installation, restart the services once to receive the events.

To modify the settings of any connector, launch Change Guardian Event Collector Addon for Windows Agent and click **Modify** against the desired collector name.

Installing Change Guardian Agent for UNIX

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

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

Prerequisite: Install the RPM `libnsl-2` if your Change Guardian is monitoring the following:

- RHEL 8.x
- Oracle Enterprise Linux 8.x
- Centos 8.x

Following sections guides you through the Change Guardian Agent for UNIX installation and configuration:

- "Interactive Installation" on page 51
- "Silent Installation" on page 52
- "Validating the Installation" on page 53

For troubleshooting information about Change Guardian Agent for UNX, see "Issues on Change Guardian Agent for UNIX" on page 233.

Interactive Installation

This section provides the following information:

- "Remote Installation" on page 51
- "Manual Installation" on page 51

Remote Installation

To install:

1. In Agent Manager click **Asset Groups > All Assets > Manage Assets > Add**.
2. From the assets list, select the machines where you want to deploy the agent.
3. Click **Manage Installation > Install Agents**.
4. Provide the `root` credentials of the machine and click **Next** and start the installation.

   If you select multiple machines, ensure that the `root` user shares the same password.

   NOTE: When you are installing Change Guardian Agent for UNIX for Change Guardian, the IP address of the Change Guardian server is automatically populated in the configuration window. If you replace the Change Guardian server in future, the new Change Guardian server must use the same IP address to maintain connection with all the agents deployed.

Manual Installation

To install:

1. Download the agent artifacts and certificates. For more information, see "Downloading the Agent Certificates and Artifacts" on page 41.
2. Log in to the machine, where you want to install the agent, with superuser privileges.
3. Click **All Assets > Manage Installation > Download**, and download the required package.

   Agent Manager downloads `ChangeGuardianAgentForUnix.zip` to your computer.
4. Extract `ChangeGuardianAgentForUnix.zip` to the computer where you want to install the Change Guardian Agent for UNIX.
5. Provide file execute permission to the `./install.sh` file and execute the `./install.sh` script.
6. Follow the prompts to complete the installation.

7 Continue with the installation steps. The installation might take a few minutes for all services to start after installation.

NOTE: Manual Installation of Change Guardian Agent for UNIX downloaded from Change Guardian Agent Manager accepts the agent certificate configuration even if there is a mismatch of the agent hostname and IP address. You must ensure that you use the correct configuration before installing Change Guardian Agent for UNIX.

Silent Installation

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

IMPORTANT: To perform silent installation, ensure that you have recorded the installation parameters during the interactive installation and then run the recorded file on other endpoints. Silent installation uses an installation file that records the information required for completing the installation. Each line in the file is a *name*=*value* pair that provides the required information, for example, `HOME=/usr/netiq`.

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

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

To install:

1 Download the installation files from the Downloads website.

2 Download the package in the `root` folder and specify the following command to extract the install files from the tar file:

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

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

3 After you create the installation file, you can run silent installation on the endpoints from command line using the following command:

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

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

NOTE: The installation process does not support Change Guardian Agent for UNIX as a non-root user.

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

Parameter	Description
FRESH_INSTALL	Specifies whether you want to install or upgrade the agent. Valid entries are 1 (install) and 0 (upgrade). The default value is 1.
CREATE_TARGET_DIR	Specifies whether you want the install program to create the target installation directory if it does not already exist. Valid entries are y and n. The default value is y.
CONTINUE_WITHOUT_PATCHES	Specifies whether the install program stops or continues when the operating system is not a supported version. Valid entries are y and n. The default value is n.
IQ_STARTUP	Specify restart method for the agent process. For information about the options, see "Validating the Installation" on page 53. Valid entries are rclink and inittab. The default option is rclink.
CGU_STARTUP	Specifies restart method for the detected process. For information about the options, see "Validating the Installation" on page 53. Valid entries are rclink and inittab. The default value is rclink.
MANAGE_AUDIT_LOGS	Specifies whether the agent reduces the size and removes old audit logs. Valid entries are y and n.
AUDIT_LOG_SIZE	Specifies the maximum size, in bytes, that the agent allows an audit log to reach before starting a new log.
AUDIT_LOG_RETENTION	Specifies the number of audit logs that the agent keeps. Once this number of audit logs exists, the agent deletes old logs when making new ones.
KEEP_OLD_AGENT_DIR	Specifies whether to keep the previous installation directory when you are upgrading the agent. Valid entries are y and n.
OLD_INSTALL_DIR_MOVED	Specifies the directory where you want the installation program to move to the previous installation directory.

Validating the Installation

To validate the installation, check if the services detectd, vigilent, auditd, and nqmagt are running:

```
ps –ef | grep -i <service_name>
```

Where *service_name* can be detectd, vigilent, auditd, or nqmagt

The output in Linux is as follows:

```
root 10447 1 0 14:39 ? 00:00:00 /usr/netiq/common/bin/nqmagt -g /usr/netiq/
common/log/nqmagt.log
root 10449 10447 0 14:39 ? 00:00:02 VigilEntAgent -config vigilent -load
va:VigilEntAdapter -d
root 135 2 0 Nov01 ? 00:00:41 [kauditd]
root 6133 1 0 Nov01 ? 00:03:12 /sbin/auditd
root 10358 1 0 14:39 ? 00:00:00 ./perl - ../local/cache/detect.xml vrun
detectd
root 10430 10358 0 14:39 ? 00:00:00 detectd[10358] -p local4.err
root 10445 10358 0 14:39 ? 00:00:00
detect_group:LinuxAuditObject__singleton
```

- `detectd`: Monitors tasks and retrieves data.
- `vigilent`: Sends events to the Change Guardian server.
- `auditd`: Writes audit records to the disk. It is an operating system service that is required by the services specific to Change Guardian Agent for UNIX. If `auditd` is not running, follow the operating system instructions to enable it.
- `nqmagt`: Monitors the status of the other agent processes and restarts them if necessary. This process should run continuously after the agent is installed.

Installing Change Guardian Configuration Scanner

Change Guardian Configuration Scanner is a standalone service that uses Windows Remote Management (WinRM) to monitor servers on a domain it is installed on, to collect configuration data and perform compliance assessments. The collection of data is governed by predefined policy templates that consist of security checks. Each security check in turn represents a specific control mandated by one or more compliance standards.

NOTE: Change Guardian Configuration Scanner does not support FIPS mode.

Setting Up The Environment

1. “Allowing Remote Server Management through WinRM” on page 54
2. “Configuring The Firewall to Allow WinRM Service” on page 55
3. “Enabling WinRM Service” on page 55
4. “Creating a WinRM Enabled User Account” on page 56
5. “Install *ASP.NET Core Runtime 5.0 (Hosting Bundle)” on page 58*

NOTE: You can create a new Group Policy Object or edit an existing one and link to apply to required member servers. Manually update group policies on target servers by using the `gpupdate /force` command or wait until group policies automatically refresh.

Allowing Remote Server Management through WinRM

1. Log in to a domain controller with domain administrator privileges.
2. Open **Group Policy Management**.

3 Navigate to the target domain.

4 Select a required Group Policy Object, right-click and select Edit to open the Group Policy Management Editor.

5 Navigate to Computer Configuration > Policies > Administrative Templates > Windows Components > Windows Remote Management (WinRM).

6 Double-click WinRM Service on the right hand pane.

6a Double-click Allow remote server management through WinRM.

6b Select Enabled and enter * as a wildcard or a range of IP addresses in the IPv4 and IPv6 filter fields

6c Click OK.

6d Double-click Disallow Kerberos authentication.

6e Select Not Configured or Disabled.

6f Click OK.

7 Select Windows Remote Shell on the left hand pane.

7a Double click Allow Remote Shell Access on the right hand pane.

7b Select Enabled.

7c Click OK.

8 Exit the Group Policy Management Editor.

Enabling WinRM Service

1 Log in to a domain controller with domain administrator privileges.

2 Open Group Policy Management.

3 Navigate to the target domain.

4 Select a required Group Policy Object, right-click and select Edit to open the Group Policy Management Editor.

5 Navigate to Computer Configuration > Preferences > Control Panel Settings > Services.

6 Right-click Services and select New > Service.

6a Select Automatic from the Startup drop-down list.

6b Enter WinRM as the Service name.

6c Select Start service from the Service Action drop-down list.

6d Click Apply and OK.

7 Exit the Group Policy Management Editor.

Configuring The Firewall to Allow WinRM Service

1 Log in to a domain controller with domain administrator privileges.

2 Open Group Policy Management.

3 Navigate to the target domain.

4 Select a required Group Policy Object, right click and select Edit to open the Group Policy Management Editor.

5 Navigate to **Computer Configuration > Policies** > **Windows Settings** > **Security Settings** > **Windows Firewall with Advanced Security** > **Windows Firewall with Advanced Security - LDAP.., Inbound Rules**.

6 Select **Inbound Rules**, right-click and select **New Rule**.

6a Select the **Predefined** radio button and then **Windows Remote Management** from the drop down list.

6b Click **Next**.

6c Keep default rule selections and click **Next**.

6d Select **Allow the connection** radio button.

6e Click **Finish**.

7 Exit the **Group Policy Management Editor**.

Creating a WinRM Enabled User Account

Change Guardian Configuration Scanner requires an Administrative user account to authenticate with WinRM service. If an Administrative account is not available, you can choose to use a least privileged user account.

To create a least privileged user account, follow the steps below:

1 Log in to a domain controller with domain administrator privileges.

2 Create a **service account** in Active Directory Users and Computers.

3 Add the created **service account** manually to the default **Remote Management Users** group on the domain controller.

4 Use **Group Policy Preferences** to add the created account to the **Remote Management Users** group of all computers across the domain:

4a Open **Group Policy Management**.

4b Navigate to the target **Domain**.

4c Select a required **Group Policy Object**, right-click and select **Edit** to open the **Group Policy Management Editor**.

4d Navigate to **Computer Configuration > Preferences > Control Panel Settings > Local Users and Groups**.

4e Right click and select **New** and then **Local Group**.

4f Select **Update** from the **Action** drop down list.

4g In the **Group Name** field, enter **Remote Management Users**.

4h Click **Add**.

4i Enter the **service account** and click **Check Names**.

4j Click **OK**.

4k Click **Apply** and **OK**.

5 Assign Registry Read permission:

5a Navigate to **Computer Configuration** > **Policies > Windows Settings > Security Settings > Registry**.

5b Complete the following steps to provide read permissions to each of the given registry keys one by one:

- MACHINE\SYSTEM\CurrentControlSet\Services\TCPIP6\Parameters
- MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\GPExtensions

5b1 Right click **Registry** and select **Add Key**.

5b2 Navigate to the required registry key and click **OK**.

5b3 Click **Add**.

5b4 Enter the **service account** and click **Check Names**.

5b5 Click **OK**.

5b6 Select the **service account** and select **Read** under the **Allow** column.

5b7 Click **Advanced**.

5b8 Select the **service account** from the **Permissions** tab.

5b9 Click **Edit**.

5b10 Select the following:

5b10a Select *Allow* from the **Type** list.

5b10b Select *This key and subkeys* from the **Applies to** list.

5b10c Click **OK** on the **Permission Entry** dialog box.

5b10d Click **OK** on the **Advanced Security Settings** dialog box.

5b10e Click **OK** on the **Security** dialog box.

5b11 Select **Configure this key then** and then **Propagate inheritable permissions to all subkeys**.

5b12 Click **OK** on the **Add Object** dialog box.

6 Assign WMI namespace permissions:

NOTE: Perform these steps on all servers Change Guardian Configuration Scanner must monitor.

6a Enter `wmimgmt.msc` in the **Run** dialog box and click **OK**.

6b Right click **WMI Control** and select **Properties**.

6c Select the **Security** tab.

6d Complete the following steps to provide required permissions to each of the given WMI namespaces and subnamespaces:

- **Root > RSOP**
- **Root > CIMV2**
- **Root > Interop**

- **Root > RSOP > Computer**
- **Root > RSOP > User**

6d1 Select and click the **Security** button.

6d2 Click **Add**.

6d3 Enter the **service account** and click **Check Names**.

6d4 Click **OK**.

6d5 Select the **service account** and then select **Allow** to enable the following permissions:

- Execute Methods
- Enable Account
- Remote Enable
- Read Security

6d6 Click **Advanced**.

6d7 Select the **service account** from the **Permissions** tab.

6d8 Click **Edit**.

6d9 Select the following:

6d9a Select *Allow* from the **Type** list.

6d9b Select *This namespace and subnamespaces* from the **Applies to** list.

6d9c Click **OK** on the **Permission Entry** dialog box.

6d9d Click **OK** on the **Advanced Security Settings** dialog box.

6d9e Click **OK** on the **Security** dialog box.

6e Click **OK** on the **WMI Control Properties** dialog box.

6f Exit the **wmimgmt** console.

Install *ASP.NET Core Runtime 5.0* (Hosting Bundle)

1. Open the ASP.NET Core download page.
2. Click Download Hosting Bundle under **Run server apps**.

Installing Change Guardian Configuration Scanner Service

Use Agent Manager to download and install Change Guardian Configuration Scanner service.

To download and install:

1. In Agent Manager, click **All Assets**> **Manage Installation**> **Download**.
2. Select the **Change Guardian Configuration Scanner** package and click **Download**.
3. Copy `ChangeGuardianConfigurationScanner.zip` to the target server and extract.
4. Copy the ChangeGuardianConfigurationScanner folder and contents to the install location, for example, `C:\Program Files`.

5. Open a **PowerShell** or **Command Prompt** as an Administrator and change the directory to the install location.
6. Use the `WSS.ConfigureService.exe` utility to execute the `Create` command to install Change Guardian Configuration Scanner service.

Using Change Guardian Configuration Scanner Commands

You can use the `WSS.ConfigureService.exe` utility as an administrator to execute commands to install and configure the Change Guardian Configuration Scanner service. The available commands are:

- Create: Creates and starts the WinRM configuration scanner service. The available options are:

  -u: The user name to authenticate with the WinRM service. This user must be an administrator or least privileged user.

  -p: The password to authenticate.

  -a: The administrator password to login to Change Guardian Configuration Scanner.

  -n: The port number for Change Guardian Configuration Scanner.

  Example:

  ```
  WSS.ConfigureService.exe Create -u ConfigScanUser -p Password -a
  AdminPassword -n 8077
  ```

- Edit: Edits WinRM credentials. The available options are:

  -u: The user name to authenticate with the WinRM service. This user must be an administrator or least privileged user.

  -p: The password to authenticate.

  -a: The administrator password to login to Change Guardian Configuration Scanner.

  Example:

  ```
  WSS.ConfigureService.exe Edit -u ChangedUser -p ChangedPassword -a
  ChangedAdminPassword -n 8077
  ```

- Import (Optional): Imports an external certificate. The available options are:

  -f: Import the external certificate(.pfx).

  -p: Enter the certificate password.

  Example:

  ```
  WSS.ConfigureService.exe Import -f PathToPFXCert -p CertPassword
  ```

- Remove: Removes Change Guardian Configuration Scanner service.

  Example:

  ```
  WSS.ConfigureService.exe Remove
  ```

Disabling Weak Cipher Suites

The ASP.NET Core Runtime server uses cipher suites of the operating system it is installed on. It is recommended to disable weak cipher suites such as RC4. To disable weak cipher suites, refer to Microsoft documentation.

Setting Up Custom User Profiles

By default, any user-related security check uses the administrator user profile. To change the user profile, follow the steps below:

1. Go to Change Guardian Configuration Scanner service Install location.
2. Open `appsettings.json` and modify the value corresponding to `UserProfileName`, from Administrator to the desired username.
3. Restart the Change Guardian Configuration Scanner service.

NOTE: Ensure to perform the preceding steps if you renamed the administrator account.

Reconfiguring the Agent

Reconfigure the agents if you have deployed the agents using Agent Manager:

To reconfigure:

1. In Agent Manger, do one of the following:
   - (Conditional) In the Agent Manager, click **All Assets** or **Approved Assets** and select the Hosts where you want to perform reconfiguration.
2. Click **Manage Installation**, and then select **Reconfigure Agents**.
3. Select the version and then select the default configuration, edit it or add a new configuration.
4. Start Reconfiguration.

Verifying After Reconfiguration

- Ensure that the service NetIQChangeGuardianAgent is running in Windows Services
- If you used Client Agent Manager, ensure that the service NetIQClientAgentManager is running in Windows Services

5 Configuring Change Guardian Server

After installing the Change Guardian server, you must perform configurations such as configure server date and time, add SMTP servers, add assets, add application licenses, and configure LDAP. This chapter provides information about using the Change Guardian server prompt, the web console, Policy Editor, and Agent Manager to perform these configurations.

- “Configurations Using Web Console” on page 61
- “Configurations Using the Server Command Prompt” on page 71
- “Configurations Using Policy Editor” on page 79
- “Configurations Using Agent Manager” on page 81

For troubleshooting information about Change Guardian server configuration, see “Issues in Change Guardian Server” on page 221.

Configurations Using Web Console

You can configure the following using the web console:

To access the web console, open the following URL:

```
https://<IP_Address_Change_Guardian_server>:<port_number>
```

The default port is 8443. You can use a custom port if Change Guardian was installed with custom configurations.

- “Adding License for Applications” on page 61
- “Configuring LDAP for AD Browsing” on page 62
- “Configuring LDAP for Authentication” on page 63
- “Creating Custom Groups” on page 65
- “Assigning Policies and Policy Sets” on page 66
- “Creating Event Routing Rules” on page 67
- “Configuring Users and Roles” on page 68

NOTE: You can configure email servers by using the server command prompt also.

Adding License for Applications

To allow Change Guardian to start monitoring, import the license key for each application.

To add or renew a license:

1. Log in to the web console, click **CONFIGURATION > Application Licenses**.
2. Click **IMPORT LICENSE KEY**.

Configuring LDAP for AD Browsing

Change Guardian provides the user name of the event initiator and the ObjectSID of an event during auditing activities. Configuring AD allows the Change Guardian server to retrieve user information from AD and map with associated incoming events. Change Guardian synchronizes AD user to provide user information associated with a particular event, such as the user name, the email address and contact details of the user.

Additionally, configuring AD with Change Guardian provides the following benefits:

- 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

Adding AD Servers

You can add, modify, delete an AD server configuration, and add a server as default from the Change Guardian web console. When you add an AD server as default, Policy Editor uses the default server and displays the objects of that server. Similarly, Agent Manager uses the server as the default server to display the list of computers when you add assets.

NOTE: You cannot configure LDAP connections in AD using Policy Editor. However, to use the configured LDAP connections in Change Guardian policies, upgrade to Policy Editor 6.2.

To add a server:

1. Click **CONFIGURATION > LDAP CONNECTIONS > ADD.**
2. Specify the required details.
   - Specify the certificate file path to allow SSL connection
   - Specify the polling interval between 30 to 120 minutes to set the interval at which Change Guardian server synchronizes all objects and groups with AD

     NOTE: In Change Guardian 6.0 and earlier, the polling interval between Change Guardian server and AD servers was hourly, weekly, or daily. For Change Guardian 6.1, the previously configured AD servers have a default polling interval is 120 minutes.
   - (Conditional) If you want to synchronize AD user profiles with Change Guardian, specify the user container details.

Adding AD servers allows you to perform the following:

- Browse AD objects when creating policies using Policy Editor.
- Manage both secured and non-secured AD servers.
- Use a domain to add multiple computers as assets using Agent Manager.

  You can install Change Guardian agents on the assets in one step using Agent Manager.
- Use AD User Container details to filter events by users names.

NOTE: When you update an AD object, the change is available with Change Guardian server after the specified polling interval has passed. Events from an updated AD object is displayed only after the interval. Similarly, you can view the updated user profiles after the interval has passed.

Mapping User Profile Fields

To synchronize AD user accounts to Change Guardian, Change Guardian needs to map the user account field names in AD 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, from the web console, click **ADMINISTRATION > Integration > AD Accounts > User Profile Mapping**.

Configuring LDAP for Authentication

You can configure a Change Guardian server for LDAP authentication to enable users to log in to Change Guardian with their LDAP directory credentials. With LDAP, Change Guardian processes each user group in a policy as group members.

You can perform LDAP authentication by either using an SSL connection or by using an unencrypted connection to the LDAP server. You can configure the Change Guardian server for LDAP authentication with or without using anonymous search on the LDAP directory:

- **Anonymous:** When you create Change Guardian LDAP user accounts, specify the directory user name. However, you do not have to specify the user distinguished name (DN).

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

  When an LDAP user logs in, the Change Guardian server authenticates the user against the LDAP directory by using the specified user DN.

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 63
- "Logging in Using LDAP User Credentials" on page 65

Setting up LDAP Authentication

To set up LDAP authentication:

1. In the web console, click **ADMINISTRATION**.
2. Click **Users > LDAP Settings**.
3. Specify the options to configure LDAP authentication:

Host: Hostname or IP address for SSL connections.

SSL: SSL connection to the LDAP server.

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

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

Specify the certificate file path when you are using an SSL connection, and if the LDAP server certificate is not signed by a well-known CA and is not trusted by default.

Anonymous Search: Option to perform anonymous searches or non-anonymous searches on the LDAP directory.

Base DN: The root container to search for users.

For example. set `o=netiq` for eDirectory.

For anonymous search, specify the root container of the LDAP directory. This is optional for eDirectory, but mandatory for Active Directory. For eDirectory, if you do not specify the Base DN, Change Guardian searches the entire directory to locate the users.

For non-anonymous search, specify the root container in the LDAP directory that contains users. This is mandatory if you are using Active Directory and if you set a domain name.

Search Attribute: The LDAP attribute having the user name to search for users.

For example, the search attribute for eDirectory is `uid` and for Active Directory it is `sAMAccountName`.

Domain Name: The Active Directory domain.

Change Guardian can perform anonymous search in Active Directory. Change Guardian uses the username@domainname (userPrincipalName) to authenticate the user before searching for the LDAP user object.

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`, Change Guardian uses the relative user DN `cn=sentinel_ldap_user` when you create an LDAP user account.

---

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

- Specify the domain name and password if you did not specify earlier. The user DN can be relative to the Base DN.
- According to LDAP standards, when you use reserved special characters as literals in a **User DN**, you must use “\”. eDirectory or Active Directory might require additional escape characters. You must use “\” as the escape character for the following scenarios:
    - A space or # occurring at the beginning of the string
    - A space occurring at the end of the string
    - Any one of the following characters: +, ", \, <, >, or ;

      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
      ```

If there is an error, review the configuration details you provided and test the connection again. To learn about the errors, examine the `/var/opt/novell/sentinel/log/server0.0.log` file.

NOTE: You must ensure that the test connection is successful before saving the LDAP settings.

---

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

Verify the configuration:

- Check that the `LdapLogin` section in 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
.ProxyLdapSSLSocketFactory"
        userProvider="ldap://10.0.0.1:636/o=netiq"
        userFilter="(&(uid={USERNAME})(objectclass=user))"
        useSSL=true;
};
```

- If you provided the LDAP server CA certificate, it is added to the `/etc/opt/novell/sentinel/config/.ldapkeystore.jks` keystore.

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 options, run the script as follows:

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

Logging in Using LDAP User Credentials

After configuring the Change Guardian server for LDAP authentication, create Change Guardian LDAP user accounts and log in to Change Guardian by using your LDAP user name and password. For more information about creating LDAP user accounts, see "Creating Users" on page 70.

Creating Custom Groups

You can create custom groups to group agents by operating systems, applications, FQDNs, or IP addresses, and so on. You can modify the filter criteria, but you cannot add or remove specific agents manually. New agents are added to a custom group depending on the filter criteria of the group.

NOTE: Change Guardian refreshes the group agents according to the specified criteria every 30 minutes.

To add:

1 Click **CONFIGURATION > Agents > Manage Custom Groups**.

2. Click the plus icon, and specify the **Group Name**.
3. Click the plus icon to specify one or more conditions.
4. Edit the condition to add the list of agents
   - Specify the FQDN to search agent names matching the FQDN
   - Specify the complete operating system name and version such as “Microsoft Windows Server 2019 Standard Edition (build 17763), 64-bit”
   - Use wildcard (Ex: 1.1.1.*) to search agents matching the IP address pattern
5. Click **SAVE**.

You can modify and delete custom groups.

Assigning Policies and Policy Sets

After creating a policy or policy set in Policy Editor, you must assign them to agents, agent groups, or both. Asset groups allow you to assign policies to the group instead of to each computer. When you add an asset to a group, Change Guardian automatically deploys the policies assigned to the group to the new asset.

Change Guardian provides the following types of asset groups:

- **Default groups:** Assets specific to platforms.

  You can view the members of default groups, but you cannot modify or delete the groups.
- **Custom groups:** Assets that match the filter criteria you specify for the group.

  NOTE: Change Guardian refreshes the group membership every 30 minutes based on the specified criteria.

  NOTE: Asset groups are now available as View Default Groups and Manage Custom Groups under Agents in the **Configuration** tab. If there is an existing static group prior to upgrade, you can create a new custom group before or after the upgrade with the same set of agents.

To assign:

1. Click **CONFIGURATION > Policies > Assign Policies**.
2. (Conditional) To assign to an agent group, click **Agent Groups** and **Default Group** or **Custom Group**, and click on the group name.
3. (Conditional) To assign to an agent, click **AGENTS** and select the agent name.
4. Click on the icon under **ASSIGN UNASSIGN**.
5. Select the policies from either **POLICY SETS**, **POLICIES**, or both, and click **APPLY**.

NOTE: You cannot assign policies using agent groups for the following asset types: Azure AD, AWS for IAM, Dell EMC, Microsoft Exchange, Microsoft Office 365.

To unassign policies or policy sets, perform the same steps and deselect the policy set or policy name.

Creating Event Routing Rules

To send email messages, you must create an event routing rule and you must configure an email serve. If you do not configure an email server, notification groups do not appear.

To create an event routing rule:

1. From the web console, click **Administration > Routing**.
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 "Configuring Email Servers" on page 72.

   The actions listed here are different than the actions displayed in the **Event Actions** tab (web console > **ADMINISTRATION**), 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.

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.

Configuring Users and Roles

You can create user roles in Change Guardian and assign them permissions. Assigning roles 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:

- "Understanding the Roles" on page 68
- "Configuring Roles" on page 68
- "Understanding Password Complexity" on page 69
- "Creating Users" on page 70

Understanding the Roles

Change Guardian has the following roles by default:

Administrator: A user in this role has administrative rights in Change Guardian. 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 Change Guardian server.

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

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. You 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 reports, rename reports, and delete report results.

NOTE: If the web console displays roles other than the listed ones, you can ignore such roles.

NOTE: If an administrator user is disabled, it results in the non-functionality of alerts.

Configuring Roles

Roles allow you to define what a user can manage and what data they can view. You can grant permissions to the role and then assign the user to the role.

To create a role:

1 In the web console, click **ADMINISTRATION**.

2 Click **Users > Users and Roles**.

3 Under **Roles**, click **Create**.

4 Specify the required information.

Review the following additional permissions that you can assign to the new role:

- **Edit knowledge base:** Allows users to view and edit the knowledge base in the **Alert Details** page
- **Manage Tags:** Allows all members to create, delete, and modify tags, and associate tags to different event sources
- **Manage roles and users**: Allows non-administrative users to administer specific roles and users
- **Proxy for Authorized Data Requestors**: Allows users to accept searches from remote data sources
- **Send events and attachments:** Allows users to send events and attachments to the server

  NOTE: You can manually assign this permission to a user who needs to forward events to the server.

- **View and execute event actions:** Allows members to view events and execute actions on the selected events
- **View detailed internal system state data:** Allows members to 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

To create users, see "Creating Users" on page 70.

Understanding Password Complexity

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 but 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 5-1 *Password Complexity Rules*

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

Validation Rule	Description
MAXIMUM_PASSWORD_LENGTH	Specifies the maximum number of characters allowed in a password.
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", 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

When you add a user in the Change Guardian, it creates an application user. You can assign roles when you create the user.

To create a user:

1. In the web console, click **ADMINISTRATION**.
2. Click **Users > Users and Roles**.
3. Under **Users**, click **Create**.

   You can use special characters to set the user name. However, the user name should be within 30 characters.

   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 69.

4 Select an authentication method:

4a (Conditional) To authenticate the user against the internal database, click **Local**.

4b (Conditional) To authenticate the user against an LDAP directory, select **Directory**.

NOTE: Ensure that you have configured the Change Guardian server for LDAP authentication. For more information, see "Configuring LDAP for Authentication" on page 63.

Configurations Using the Server Command Prompt

This section provides the following information:

- "Configuring Memory Settings" on page 71
- "Configuring Server Date and Time Synchronization" on page 71
- "Verifying Server Hostname" on page 72
- "Configuring Email Servers" on page 72
- "Configuring Email Server to Receive Email Alerts" on page 73
- "Configuring Security Settings" on page 73
- "Configuring FIPS 140-2" on page 77

Configuring Memory Settings

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

To change the kernel SHMMAX parameter, append the following information to the `/etc/sysctl.conf` file:

```
# for Postgresql
kernel.shmmax=1073741824
```

NOTE: By default, in RHEL SHMMAX is a low value, 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 and time with an external time service, configure NTP.

Verifying Server Hostname

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

1. Verify the hostname configuration:

   ```
   cat /etc/HOSTNAME
   ```

2. Check the server hostname setting:

   ```
   hostname -f
   ```

3. Verify the DHCP configuration:

   ```
   cat /etc/sysconfig/network/dhcp
   ```

   NOTE: The `DHCLIENT_HOSTNAME_OPTION` setting should reflect the fully-qualified hostname of the Change Guardian server.

4. Resolve the hostname to the IP address:

   ```
   nslookup FULLY_QUALIFIED_HOSTNAME
   ```

5. Resolve the server hostname from the client by running the following command entered from the remote server:

   ```
   nslookup FULLY_QUALIFIED_CHANGEGUARDIANSERVER_HOSTNAME
   ```

Configuring Email Servers

Complete the following steps to configure SMTP:

- "Configuring Email Server With Change Guardian in FIPS Mode" on page 72
- "Configuring Email Server With Change Guardian in Non-FIPS Mode" on page 73

You can also configure email servers by using Policy Editor.

Configuring Email Server With Change Guardian in FIPS Mode

To configure:

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 by running the following command:

   ```
   ./convert_to_fips.sh -i <certificate_path>
   ```

   NOTE: If the certificate is not available in the current directory /opt/ novell/ sentinel/ bin, it is not added in the keystore database.

4. Restart the Change Guardian server using the following command:

   ```
   rcsentinel restart
   ```

Configuring Email Server With Change Guardian in Non-FIPS Mode

To configure:

1. Export the certificate from the respective SMTP server site.
2. Import the certificate:

   ```
   /opt/novell/sentinel/jdk/jre/bin/keytool
   ```

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

3. Restart the Change Guardian server:

   ```
   rcsentinel restart
   ```

Configuring Email Server to Receive Email Alerts

To receive alerts on emails, complete the following steps:

1. Add Email Servers.
2. Create Notification Groups.
3. Create Event Routing Rule to send emails.

Adding Email Servers

To add email servers to Change Guardian server and change the default email host settings:

1. Change directory:

   ```
   cd /opt/netiq/cg/scripts
   ```

2. Set the email host settings:

   ```
   ./configure.sh udei --admin-account=<admin_account> --admin-
   password=<admin_account_password>  --mail-host=<SMTP_hostname>  --mail-
   port=<SMTP_port>  --mail-from=<e-mail_address>   --secure-
   connection=<true/false>
   ```

NOTE: To configure secure connection with STARTTLS, set the following option:

```
--secure-connection=true
```

Configuring Security Settings

This section provides the following information:

- "Using CA Signed Certificates" on page 74
- "Applying Updates for Security Vulnerabilities in Embedded Third-Party Products" on page 77

Using CA Signed Certificates

You can replace the self-signed certificate with a certificate signed by a well-known CA, such as VeriSign, Thawte, or Entrust. You can also replace the self-signed certificate with a certificate digitally signed by a less common CA, such as a CA within your company or organization.

NOTE: There are many well-known CAs and identifying which CAs are most commonly used varies with country.

This section provides information about various certificates used in Change Guardian and instructions about configuring the TLS/SSL certificates to get them digitally signed by a CA:

- Types of Certificates
  - Web Server Certificate
  - Javos and Agent Manager
- Configuring the TLS/ SSL Certificates
  - Web Server Certificate
  - Javos and AMS Certificates

Web Server Certificate

The web server certificate is used for the following purposes:

- With web browsers to connect to the Change Guardian Main interface.
- Establish trust relationships for the REST API calls between Change Guardian instances. For example, it is used when configuring Data Federation

Javos and Agent Manager

The Javos and Agent Manager certificates are used for the following purposes:

- Javos certificates are used for accepting connections from Change Guardian Agents.
- Agent Manager certificates are used for communicating Change Guardian agents with Agent Manager.

Configuring the TLS/ SSL Certificates for Web Server

Configuring the TLS/SSL certificates involves the following steps:

- Generating a Certificate Signing Request
- Getting the CSR Signed by the CA
- Importing the Digitally Signed Certificates into Change Guardian

Generating a Certificate Signing Request

To obtain a digitally signed certificate, you must first generate a certificate signing request (CSR), which is presented to the CA. To generate one or more CSRs, perform the following steps on the Change Guardian server:

1 Log in to the Change Guardian server as the novell user.

2 Create a certificate pair by using the following command:

```
/opt/novell/sentinel/jdk/jre/bin/keytool -genkey -alias webserver -
validity <days> -storetype JKS -keyalg RSA -keysize 2048 -storepass
password -keypass password -keystore .webserverkeystore.jks -dname
"CN=<certificate_common_name>,OU=<organization_unit>, O=<organization>,
L=<city or town>, ST=<state>, C=<country>" -ext san=dns:<domain_name>
&& /opt/novell/sentinel/jdk/jre/bin/keytool -certreq -alias webserver -
file .webserverkeystore.csr -keystore .webserverkeystore.jks -storepass
password -ext san=dns:<domain_name>
```

The above command generates a CSR using the PKCS#10 format. The certificate signing requests are now saved in the specified file.

Getting the CSR Signed by the CA

1 Submit the CSRs to the CA for signature.

2 Obtain the signed certificate files from the CA.

The details of how this is done depend on the CA. For more information, consult your CA.

Importing the Digitally Signed Certificates into Change Guardian

Copy the files that contains the digital certificates signed by the CA to the Change Guardian server. If the files are signed by an enterprise or organizational CA rather than a well-known CA, you must copy the CA's self-signed root certificate to the Change Guardian server. You must import the intermediate, root, and signed certificates.

You can specify the desired alias names for the intermediate and root certificates. However, the signed certificate must be imported with the same alias that was used while creating a certificate pair, which is webserver. The default keystore password is *password*. If you have changed the keystore password, specify the changed password.

To import the certificate files to the Change Guardian server:

1 Log in to the Change Guardian server as the novell user.

2 Back up the default self-signed certificate:

```
cp /etc/opt/novell/sentinel/config/.webserverkeystore.jks /etc/opt/
novell/sentinel/config/.webserverkeystore.jks_bkp
```

3 Copy the CA signed certificate to the Sentinel server:

```
cp <CA_signed_certificate> /etc/opt/novell/sentinel/config/
.webserverkeystore.jks
```

4 Import the intermediate certificate:

```
/opt/novell/sentinel/jdk/jre/bin/keytool -importcert -alias
<alias_name> -file /opt/cert/intermediate.pem -keystore /etc/opt/
novell/sentinel/config/.webserverkeystore.jks -storepass
<keystore_password>
```

5 Import the root certificate:

```
/opt/novell/sentinel/jdk/jre/bin/keytool -importcert -alias
<alias_name> -file /opt/cert/root.pem -keystore /etc/opt/novell/
sentinel/config/.webserverkeystore.jks -storepass <keystore_password>
```

6 Import the signed certificate:

```
/opt/novell/sentinel/jdk/jre/bin/keytool -importcert -alias webserver -
file /opt/cert/signedcert.pem -keystore /etc/opt/novell/sentinel/
config/.webserverkeystore.jks -storepass <keystore_password>
```

7 (Optional) Verify whether all the certificates are imported successfully:

```
/opt/novell/sentinel/jdk/jre/bin/keytool -list -keystore /etc/opt/
novell/sentinel/config/.webserverkeystore.jks
```

8 Restart Change Guardian:

```
rcsentinel restart
```

Configuring the TLS/ SSL Certificates for Javos and Agent Manager

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

To replace the self-signed certificates on the server:

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

2 Switch user to `novell`.

3 Backup of the existing `certs` folder, which is located at `/opt/netiq/cgutils/certs`.

4 Create a new `certs` folder at `/opt/netiq/cgutils/`.

5 Copy the CA-signed certificates to `/opt/netiq/cgutils/certs`.

6 Change the permission of the `certs` folder:

```
chmod 700 /opt/netiq/cgutils/certs
```

7 Rename the CA-signed certificate files as below:

- `cgca-cert.pem`: Root CA certificate
- `cgca-pk.pem`: Private key
- `cgca-pk.pem.pass`: Private key password

8 Change the ownership of the CA-signed files:

```
chown novell:novell /opt/netiq/cgutils/certs/*
```

9 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.

10 Verify that the new certificates have the new CA name in the issuer field:

- `openssl x509 -in amsca-cert.pem -noout -text`
- `openssl x509 -in javosca-cert.pem -noout -text`

11 Go to the `/opt/netiq/ams/ams/bin` directory, and run the following commands:

```
./ams_cert_setup.sh --setup --profile=ams_new_profile_name
./ams_cert_setup.sh --enable --profile=ams_new_profile_name
```

NOTE: Consider not changing default profile names and create profile with a new name.

12 Confirm that the profile is enabled:

```
./ams_cert_setup.sh --show
```

13 Go to the `/opt/netiq/cg/javos/bin/` directory and run the following commands:

```
./javos_cert_setup.sh --setup --profile=javos_new_profile_name
./javos_cert_setup.sh --enable --profile=javos_new_profile_name
```

14 Confirm that the profile is enabled:

```
./javos_cert_setup.sh --show
```

15 (Conditional) If the Change Guardian server is in FIPS mode, run the following commands:

```
./opt/netiq/ams/ams/bin/convert_to_fips.sh
./opt/netiq/cg/javos/bin/convert_to_fips.sh
```

16 (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 security vulnerabilities (CVE) for these products with Change Guardian releases.

The third-party products have their own release cycles and new CVEs might be discovered before a Change Guardian release. You must review the CVEs for each embedded third-party product and decide whether to apply these updates to your Change Guardian deployment before getting a corresponding Change Guardian patch from Micro Focus. If you decide to apply patches to address these CVEs, contact Technical Support.

Configuring FIPS 140-2

Change Guardian offers enhanced protection against security threats and compliance with United States federal government standards by supporting 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 re-certified by Common Criteria at EAL3+ and provides FIPS 140-2 Inside.

Complete the following steps to configure FIPS:

1. Convert Change Guardian server to FIPS

2. Convert javos services to FIPS
3. Convert ams service to FIPS

To convert Change Guardian server:

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

2 (Conditional) If you want to change the keystore password:

2a At the Change Guardian server command prompt, switch to `novell` user.

2b Change directory to <*installation_directory*>`/opt/novell/sentinel/bin`, and run the following command: `./chg_keystore_pass.sh`

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

3 Switch to `root` user.

4 Change directory to <*installation_directory*>`/opt/novell/sentinel/bin`, and run the following command:

```
./convert_to_fips.sh
```

4a Specify n to backup the server.

4b Provide a password that meets the stated criteria. This password is required later during this procedure.

4c Specify y to insert external certificates in the keystore database.

5 Specify the path of the Elasticsearch certificate:

```
<installation_directory>/opt/novell/sentinel/3rdparty/elasticsearch/
config/http.pks
```

6 Specify the alias name of the certificate.

7 Specify y to restart the Sentinel server.

8 Ensure that the file <*installation_directory*>`/var/opt/novell/sentinel/log/server0.0.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":"vosres
tdispatcher:rest
```

To convert javos services:

1 Change directory to <*installation_directory*>`/opt/netiq/cg/javos/bin`, and run the following command:

```
./convert_to_fips.sh
```

1a Provide the password for the FIPS keystore database (the password you created in Step 4b on page 78).

1b When prompted to restart the javos service, select y.

2. Ensure that the following entry is present in the <*installation_directory*>/opt/netiq/cg/javos/log/javos.log file:

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

To convert ams service:

1. Change directory to <*installation_directory*>/opt/netiq/ams/ams/bin, and run the following command:

```
./convert_to_fips.sh
```

1a Specify a password for the FIPS keystore database.

1b When prompted to restart the Agent Manager service, select y.

2. Ensure that the <*installation_directory*>/opt/netiq/ams/ams/log/ams.log file 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. <installation_directory>/opt/netiq/ams/ams/security/nss
```

Configurations Using Policy Editor

Use Policy Editor to perform the following tasks:

- "Adding Email Servers to Change Guardian" on page 79
- "Creating and Configuring Notification Groups" on page 80

Adding Email Servers to Change Guardian

Ensure each event destination computer in your Change Guardian environment hosts an email server. Then you can add each email server to Change Guardian. Change Guardian can send email notifications to specified administrators and operators.

You can also configure email servers by using the Change Guardian command prompt.

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.
   - **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** is set to **25** by default.

- **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 (using the **ADMINISTRATION** tab in the web console), you can choose from the notification groups available for that email server. For more information, see "Creating Event Routing Rules" on page 67.

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 email contains the details of the change detected by Change Guardian.
   - **Email Format**: Specifies either text or HTML.

Configurations Using Agent Manager

You can use Agent Manager to manage assets, install agents on the assets, apply agent packages, and collect agent logs. This section provides the following information:

- "Adding Assets" on page 81

For troubleshooting information, see "Issues in Agent Manager" on page 231.

Adding Assets

An asset is a device that you can monitor using Change Guardian.

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 asset group. Asset groups allow you to assign policies to the group instead of to each individual computer. When you add an asset to a group, Change Guardian automatically deploys the policies assigned to the group to the new asset.

To add assets:

1. Open the following URL:

   `https://<IP_Address_Change_Guardian_server>:<port_number>`

   The default port is 8443. You can use a custom port if Change Guardian was installed with custom configurations.
2. In the web console, click **AGENTS**.
3. Click **All Assets > Manage Assets > Add**.
4. (Conditional) To import assets from an Active Directory server, use the **Active Directory** tab.

   NOTE: If you are using Active Directory over SSL or TLS connection, ensure that you have imported the Active Directory SSL certificate to the Change Guardian server. For more information, see "Using CA Signed Certificates" on page 74.
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, and use a tab to separate the columns. In the Hostname column, specify the fully-qualified domain names of the computers where you want to deploy agents. Optionally, you can specify the IP addresses under 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.

You can move an asset from one group to another:

- To move an asset to **Approved asset**, check whether the Client Agent Manager service is communicating with Agent Management Service.
- To move assets from **Assets not in any group** to any user defined group, select the asset, go to **Manage Asset > Move Assets to a Group**, and then select the required group.
- To organize and manage assets, create asset groups under **User defined groups** and copy assets from **Approved Assets** group to **User defined groups**.

6 Setting Up Assets For Monitoring

Change Guardian monitors events of your assets such as Windows Active Directory, Group Policy, Windows, and so on. Change Guardian provides monitoring of specified asset objects. There are Change Guardian policies for each asset type that you can use to monitor the asset objects.

Configure assets to allow Change Guardian agents to collect events from the assets.

This section provides information about configuring the following assets:

Configuring Windows Active Directory Monitoring

Change Guardian monitors the following in Active Directory (AD):

- AD objects
- AD Query
- Computer accounts
- Configurations
- Contacts
- DNS Configuration
- Federation Service
- Groups
- Organization units
- Schema
- Trusts
- User accounts

This chapter provides information about the following:

- "Implementation Checklist" on page 84
- "Prerequisites" on page 84
- "Categories of Change Guardian Policies for Windows Active Directory" on page 88

Implementation Checklist

Complete the following tasks to start monitoring Windows Active Directory audit events:

Task	See
Review requirements and recommendations for computers running the AD Domain Service	Change Guardian System Requirements
Complete the prerequisites	"Prerequisites" on page 84
Add the license key	"Adding License for Applications" on page 61
Configure Change Guardian for monitoring	"Categories of Change Guardian Policies for Windows Active Directory" on page 88
	"Assigning Policies and Policy Sets" on page 126
Triage events	Chapter 8, "Configuring Events," on page 129
	Chapter 9, "Configuring Alerts," on page 135

Prerequisites

Ensure that you have completed the following:

- Install Change Guardian Agent for Windows
- Install Policy Editor
- Configure Active Directory

Configuring Active Directory

Complete the following tasks to allow Change Guardian to monitor Active Directory events.

NOTE: Change Guardian documentation provides the third-party configuration steps for ease of use. For more information about the third-party products or for any issues with the configuration, see their documentation.

- "Configuring the Security Event Log" on page 85
- "Configuring AD Auditing" on page 85
- "Configuring User and Group Auditing" on page 86
- "Configuring Security Access Control Lists" on page 87

NOTE: Ensure that you have the required permission to complete these tasks. Check with your network or system administrator for assistance.

Configuring the Security Event Log

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

To configure the security event log:

1. Log in as an administrator to a computer in the domain that you want to configure.
2. To open Group Policy Management Console, enter the following at the command prompt: `gpmc.msc`
3. Open **Forest > Domains** > ***domainName***> **Domain Controllers**.
4. Right-click **Default Domain Controllers Policy**, and then click **Edit**.

   NOTE: Changing 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 set:
   - **Maximum security log size** to 10240 KB (10 MB) or more
   - **Retention method for security log** to **Overwrite events as needed**
7. To update policy settings, run the `gpUpdate` command at the command prompt.

To verify the configuration is successful:

1. Open a command prompt as an administrator to the computer.
2. Start Event Viewer: `eventvwr`
3. Under Windows logs, right-click **Security**, and select **Properties**.
4. Ensure that the settings show maximum log size of 10240 KB (10 MB) or more and that “Overwrite events as needed” is selected.

Configuring AD Auditing

Configure AD auditing to enable logging of AD events in the security event log.

Configure Default Domain Controllers Policy GPO with Audit Directory service access to monitor both success and failure events.

To configure AD auditing:

1. Log in as an administrator to a computer in the domain that you want to configure.
2. To open Group Policy Management Console, run `gpmc.msc` at the command prompt.
3. Expand **Forest > Domains** > ***domainName*** > **Domain Controllers**.

4. Right-click **Default Domain Controllers Policy**, and click **Edit**.

   NOTE: Changing 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 > Advanced Audit Policy Configuration > Audit Policies**.

   5a To configure AD and Group Policy, under **Account Management**, and **Policy Change**, select the following for each subcategory: **Configure the following audit events**, **Success**, and **Failure**.

   5b To configure only AD, under **DS Access**, select the following for each subcategory: **Configure the following audit events**, **Success**, and **Failure**.

6. Expand **Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Audit Policy**.

   6a For each of the following policies, select **Define these policy settings**, **Success**, and **Failure** in the **Security Policy Setting** tab:

   - **Audit account management**
   - **Audit directory service access**
   - **Audit policy change**

7. To update policy settings, run the `gpUpdate` command at the command prompt.

For more information, see *Monitoring Active Directory for Signs of Compromise* in the Microsoft Documentation site.

Configuring User and Group Auditing

Configure user and group auditing to audit the following activities:

- Logon and logoff activities of local users and Active Directory users
- Local user settings
- Local group settings

To configure user and group auditing:

1. Log in as an administrator to a computer in the domain that you want to configure.
2. Open Microsoft Management Console, select **File > Add/Remove Snap-in**.
3. Select **Group Policy Management Editor** and click **Add**.
4. In 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**.

7. In the Microsoft Management Console, expand **Default Domain Controllers Policy *FQDN* > Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Audit Policy**.
8. Under **Audit Account Logon Events** and **Audit Logon Events**, select **Define these policy settings**, **Success**, and **Failure**.
9. 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**.
10. Under **Audit Logon**, select **Audit Logon**, **Success**, and **Failure**.
11. Under **Audit Logoff**, select **Audit Logoff**, **Success**, and **Failure**.
12. To update policy settings, run the `gpupdate /force` command at the command prompt.

Configuring Security Access Control Lists

Security Access Control Lists (SACLs) describe the objects and operations to monitor.

To allow Change Guardian to monitor changes of current and future objects inside Active Directory, follow the steps in "Configuring SACLs for AD" on page 87. However, if you are using Change Guardian for only Group Policy in your environment, see "Configuring SACLs for GPO" on page 91.

Configuring SACLs for AD

To monitor all changes of current and future objects inside Active Directory, configure the domain node.

To configure SACLs:

1. Log in as an administrator to a computer in the domain that you want to configure.
2. To open ADSI Edit configuration tool, run `adsiedit.msc` at the command prompt.
3. Right-click **ADSI Edit**, and select **Connect to**.
4. In the Connection Settings window, specify the following:
   - **Name** as `Default naming context`.
   - **Path** to the domain to configure.
   - If you are performing this step for the first time, select **Default naming context**.
   - If you are performing for the second time, select **Schema.**
   - If you are performing for the third time, select **Configuration**.

   NOTE: You must perform Step 4 through Step 11 three times, to configure connection points for **Default naming context**, **Schema**, and **Configuration**.

5. In **Connection Point**, set **Select a well known Naming Context** to **Default naming context**.
6. In the ADSI Edit window, expand **Default naming context**.
7. Right-click the node under the connection point (begins with DC= or CN=), and click **Properties**.
8. On the **Security** tab, click **Advanced > Auditing > Add**.
9. In **Applies to** or **Apply onto**, select **This object and all descendant objects**.

10 Configure auditing to monitor every user:

10a Click **Select a principal**, and type `everyone` in **Enter the object name to select**.

10b Specify the following options:

- **Type** as **All**
- Select **Permissions** as:
  - **Write All Properties**
  - **Delete**
  - **Modify Permissions**
  - **Modify Owner**
  - **Create All Child Objects**

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

    The other nodes related to child objects are selected automatically

11 Deselect the option **Apply these auditing entries to objects and/or containers within this container only**.

12 Repeat Step 4 through Step 11 two more times.

Categories of Change Guardian Policies for Windows Active Directory

AD objects: Policies about creating and deleting a domain, modifying connection object, and so on

Computer accounts: Policies about disabling and moving a computer account, and changing permission to accounts

Configurations: Policies about creating and deleting GPOs

Contacts: Policies about creating, deleting, moving, and changing permission of contacts

DNS Configuration: Policies about modifying DNS configurations, and monitoring the node and zone

Groups: Policies about the following:

- Creating distribution group and security group
- Membership changes to distribution group, privilege group, and security group

Organization units: Policies about creating, deleting, moving, and changing permission of organization unit

Schema: Policies about the following:

- Creating and changing schema attributes and classes
- Deactivating and reactivating schema objects
- Changing schema permissions
- Changing schema settings

NOTE: If you want to receive all events related to Schema, create more than one policy having related Schema events as policy definition. For example, create a policy to monitor events about schema attribute created and schema attribute modified.

Trusts: Policies about creating, deleting, and modifying trust

User accounts: Policies about the following:

- Changing administrator or guest accounts
- Failure to reset user password
- Disabling and moving user accounts
- Changing permission to user accounts

For more information about creating policies, see "Creating Policies" on page 124.

After creating policies, you can assign them to assets. For information about assigning policies, see "Assigning Policies and Policy Sets" on page 66.

NOTE: If you assign the Active Directory schema policies created for Attribute and Class schema monitoring together, the AD schema events are not generated successfully. Create separate policies for Attribute and Class schema.

Configuring Windows Active Directory Federation Services Monitoring

Change Guardian monitors the following in Active Directory Federation Services (ADFS):

- Application token failure/success
- Fresh credential validation success/failure
- Password change request success/failure

Configuring ADFS Auditing

- "Configure ADFS auditing to enable logging of ADFS events in the security event log" on page 89
- "Configure auditing for ADFS in the ADFS Management snap-in" on page 90

Configure ADFS auditing to enable logging of ADFS events in the security event log

To configure ADFS auditing:

1. Log in as an administrator in the domain that you want to configure.
2. Open **Group Policy Management Console**. Run `gpmc.msc` using command prompt.
3. Click **Forest** > **Domains** > **Domain Name** > **Domain Controllers**.
4. Right-click **Default Domain Controllers Policy** and select **Edit**.

NOTE: Changing 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. Click **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Advanced Audit Policy Configuration** > **Audit Policies**.
6. To configure ADFS auditing under **Object Access**, select the following for Audit Application Generated: **Configure the following audit events**, **Success**, and **Failure**.
7. To update policy settings, run the `gpUpdate` command at the command prompt

Configure auditing for ADFS in the ADFS Management snap-in

1. To open ADFS Management snap-in, navigate to **Programs** > **Administrative Tools** > **ADFS Management**
2. Click **Actions** and select **Edit Federation Service Properties**.
3. In the dialog box that opens, click on the **Events** tab. Enable it for **Success** and **Failure**.

Configuring Group Policy Monitoring

Change Guardian monitors the following in Group Policy:

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

This section provides the following information:

- "Implementation Checklist" on page 90
- "Prerequisites" on page 91
- "Categories of Change Guardian Policies for GPO" on page 92

Implementation Checklist

Complete the following tasks to start monitoring Group Policy events:

Task	See
Complete the prerequisites	"Prerequisites" on page 91
Add the license key	"Adding License for Applications" on page 61

Task	See
Configure Change Guardian	“Categories of Change Guardian Policies for GPO” on page 92
	“Assigning Policies and Policy Sets” on page 126
Triage events	Chapter 8, “Configuring Events,” on page 129
	Chapter 9, “Configuring Alerts,” on page 135

Prerequisites

Ensure that you have completed the following:

- Install Change Guardian Agent for Windows
- Install Policy Editor
- Configure GPO

Configuring GPO

Complete the following tasks to configure Change Guardian server to monitor GPO events.

NOTE: Change Guardian documentation provides the third-party configuration steps for ease of use. For more information about the third-party products or for any issues with the configuration, see their documentation.

- “Configuring the Security Event Log” on page 85
- “Configuring AD Auditing” on page 85
- “Configuring SACLs for GPO” on page 91

NOTE: Ensure that you have the required permission to complete these tasks. Check with your network or system administrator for assistance.

Configuring SACLs for GPO

Configure SACL to generate events for operations that can result in, or are related to, changes in GPO data stored in Active Directory.

To configuration SACL:

1. Log in as an administrator to the computer in the domain you want to configure.
2. To open ADSI Edit configuration tool, run `adsiedit.msc` at the command prompt.
3. Right-click **ADSI Edit**, and then select **Connect to**.
4. In the Connection Settings window, specify the following:
    - **Name** as `Default naming context.`
    - **Path** to the domain to configure.
    - If you are performing this step for the first time, select **Default naming context**.

- If you are performing for the second time, select **Schema.**
- If you are performing for the third time, select **Configuration**.

5 In **Connection Point**, set **Select a well known Naming Context** to **Default naming context**.

6 In the ADSI Edit window, expand **Default naming context**.

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

8 On the **Security** tab, click **Advanced > Auditing > Add**.

9 Configure auditing to monitor every user:

   9a Click **Select a principal** and type `everyone` in **Enter the object name to select**.

   9b Specify the following options:

   - **Type** as **All**
   - Select **Permissions** as:
     - **Delete**
     - **Create Organizational Unit objects**
   - Select **Properties** as:
     - **Write gPLink**
     - **Write gPOptions**

10 Deselect the option **Apply these auditing entries to objects and/or containers within this container only**.

11 In **Connection Point**, select **Select a well known Naming Context**, and **Configuration**.

12 Expand **Configuration**.

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

14 On the **Security** tab, click **Advanced > Auditing > Add**.

15 Configure auditing to monitor every user:

   15a Click **Select a principal** and type `everyone` in **Enter the object name to select**.

   15b Specify the following options:

   - **Type** as **All**
   - Select **Permissions** as:
     - **Delete**
     - **Create Sites Container objects**
   - Select **Properties** as:
     - **Write gPLink**
     - **Write gPOptions**

16 Deselect **Apply these auditing entries to objects and/or containers within this container only**.

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

Categories of Change Guardian Policies for GPO

Group Policy Objects: Policies about deleting and modifying group policies and domain policies

Group Policy Preferences: Policies about changes to local user and group preferences to GPO

Group Policy Settings: Policies about modifying software settings

Starter Group Policy Objects: Policies about creating, deleting, and modifying starter group policies

SYSVOL: Policies about changing Central Store and SYSVOL folder

For information about creating policies, see "Creating Policies" on page 124.

After creating policies, you can assign them to assets. For information about assigning policies, see "Working with Policies" on page 125.

Configuring Windows Monitoring

Change Guardian monitors the following in Windows:

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

This section provides the following information:

- "Implementation Checklist" on page 93
- "Prerequisites" on page 94
- "Categories of Change Guardian Policies for Windows" on page 94

Implementation Checklist

Complete the following tasks to start monitoring Windows events:

Task	See
Complete the prerequisites	"Prerequisites" on page 94
Add a license key	"Adding License for Applications" on page 61
Configure Change Guardian for monitoring	"Categories of Change Guardian Policies for Windows" on page 94
	"Assigning Policies and Policy Sets" on page 126
Triage events	Chapter 8, "Configuring Events," on page 129
	Chapter 9, "Configuring Alerts," on page 135

NOTE: Change Guardian monitors 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.

Prerequisites

Ensure that you have completed the following:

- Install Change Guardian Agent for Windows
- Install Policy Editor

Categories of Change Guardian Policies for Windows

File integrity: Policies about changes to critical startup file

File shares: Policies about creating file shares and monitoring permission changes

File systems: Policies about monitoring binary files and permission changes to system directories, privileged profiles, and security analysis database

Local users and groups: Policies about the following:

- Changes to administrator group membership and administrator group privileges
- Creating, deleting user account, and changes to password
- Enabling, disabling, modifying administrator, and changing administrator privilege

Processes: Policies about executing undesirable processes

Registry: Policies about changes to application installation, changes to service registration, and so on.

Removable media: Policies about attaching removable media and file writing to the removable media

For Change Guardian to monitor the registry enable the Registry Browser. Set the `HKLM\Software\Wow6432Node\NetIQ\ChangeGuardianAgent\repositoryEnabled` flag to 1 and restart the agent. If you do not manually set the flag to 1, Registry Browser displays the error message: “Could not connect to Windows Data Source.”

To create a policy to monitor Local Users and Groups, in Policy Definition, select **event list**, or **Privilegelist**, or both.

For information about creating policies, see “Creating Policies” on page 124.

After creating policies, you can assign them to assets. For information about assigning policies, see “Assigning Policies and Policy Sets” on page 66.

Configuring Microsoft Azure Active Directory Monitoring

Microsoft Azure Active Directory (Azure AD) is a cloud-based directory and identity management service. Change Guardian allows you to monitor Azure AD along with on-premises Active Directory.

The Azure AD monitoring capability in Change Guardian is built in with Microsoft Graph API.

Change Guardian monitors the following in Azure AD:

- Administrative units

- Applications
- Devices
- Directories
- Groups
- Policies
- User accounts

This section provides the following information:

- “Implementation Checklist” on page 95
- “Prerequisites” on page 96
- “Configuring Change Guardian for Monitoring” on page 98
- “Categories of Change Guardian Policies for Azure AD” on page 99

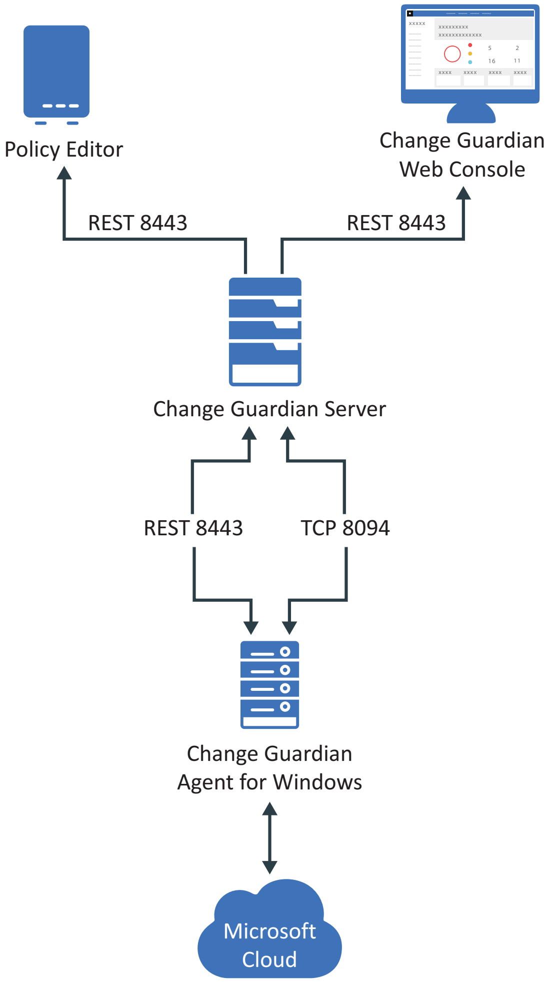
Implementation Checklist

Complete the following tasks to start monitoring Azure AD audit events:

Task	See
Complete the prerequisites	“Prerequisites” on page 96
Add the license key	“Adding License for Applications” on page 61
Configure Change Guardian for monitoring	“Categories of Change Guardian Policies for Azure AD” on page 99 “Assigning Policies and Policy Sets” on page 66
Triage events.	Chapter 8, “Configuring Events,” on page 129 Chapter 9, “Configuring Alerts,” on page 135

The following illustration explains the workflow of various components with Azure AD:

Figure 6-1 Azure AD Monitoring using Change Guardian



The deployment diagram illustrates the following:

- Change Guardian Agent for Windows collects events from Azure AD
- Change Guardian Agent for Windows sends the event details to the Change Guardian server

Prerequisites

Ensure that you have completed the following:

- Install Change Guardian Agent for Windows
- Install Policy Editor
- Configure Default Windows Registry Keys

Configuring Default Windows Registry Keys

Change Guardian has defined the default values for the Windows registry keys. To modify the registry key values, see the following sections:

NOTE: Change Guardian documentation provides the third-party configuration steps for ease of use. For more information about the third-party products or for any issues with the configuration, see their documentation.

- "Configuring Azure AD Event Fetching Interval" on page 97
- "Configuring Azure AD Access Token Refresh Time Interval" on page 97
- "Configuring Azure AD Event Collection Interval" on page 98

NOTE: Ensure that you have the required permission to complete these tasks. Check with your network or system administrator for assistance.

Configuring Azure AD Event Fetching Interval

Change Guardian fetches events at a given time interval. The default interval is set to 120 minutes. If the agent starts at 10 a.m., event fetching starts 120 minutes before the *current system time*, that is, from 8 a.m. to 10 a.m.

WARNING: If the time interval is set to more than 1440 minutes, the system resets it to 1440 minutes automatically because it is the maximum permitted value. If the latency from Microsoft is more than this value, there might be data loss.

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

While processing Azure AD events, Change Guardian removes duplicate events. For more information, see Azure Active Directory reporting latencies.

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. Under **Base**, select **Decimal**.
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 and 1440 minutes.
5. Go to **Services > NetIQ Change Guardian Agent**.
6. Select the Change Guardian Agent for Windows application, and click **Restart**.

Configuring Azure AD Access Token Refresh Time Interval

Access token is the interval at which Change Guardian connects to Azure AD. By default, Change Guardian refreshes the access token every 30 minutes with a maximum interval of 50 minutes. If you configure this value below 15 minutes or above 50 minutes, the system automatically resets to either 15 or 50 minutes respectively.

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 `AzureADTokenRefreshInterval` key.
3. Select **Decimal** under **Base**.
4. Specify the time interval to any required value range between 15 minutes and 50 minutes.
5. Go to **Services > NetIQ Change Guardian Agent**.
6. 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 Azure AD and processes them based on applied AD policies.

You can configure the event collection interval to be any duration between 5 minutes and 30 minutes. If you configure the duration to below 5 minutes or above 30 minutes, the system automatically resets it either to 15 or 30 minutes respectively. However, you can consider a fetch interval of 10 minutes.

To modify this 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 `AzureADEventCollectionInterval` key.
3. Select **Decimal** under **Base**.
4. Specify the time interval to any required value range between 5 minutes and 30 minutes.
5. Go to **Services** > **NetIQ Change Guardian Agent**.
6. Select the Change Guardian Agent for Windows application, then click **Restart**.

Configuring Change Guardian for Monitoring

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

- “Enabling Azure AD Monitoring” on page 98
- “Configuring Azure AD Tenant” on page 99

Enabling Azure AD Monitoring

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

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

To reconfigure:

1. In Agent Manager, select the asset and click **Manage Installations > Reconfigure Agents**.
2. On the Reconfigure Agents page, select **Enable Azure AD Monitoring** under **Edit Agent Configuration**.

Configuring Azure AD Tenant

In 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 to make it available to Change Guardian. Change Guardian connects with Azure AD using the Microsoft Graph API. It supports a single tenant.

To configure the Azure AD tenant:

1. Log in to Policy Editor.
2. Under **Azure AD**, open **Azure Tenant Configuration**.
3. Specify values for the following fields:
   - **Domain Name**: Specify the name of the Azure AD 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.

Categories of Change Guardian Policies for Azure AD

Administrative Unit: Policies about adding, deleting, and updating administrative units, and modifying administrative unit attributes

Applications: Policies about adding, deleting, and updating applications and application owners

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

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

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

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

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

For information about creating Azure AD policies, see "Creating a Policy for Azure AD Groups" on page 99. For information about creating policies in Change Guardian, see "Creating Policies" on page 124.

After creating policies, you can assign them to assets. For information about assigning policies, see "Assigning Policies and Policy Sets" on page 66.

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

Creating a Policy for Azure AD Groups

To create a policy:

1. In Policy Editor, select **Azure AD > Azure AD Policies**.

2 Select **Groups** and specify the information in the Groups Policy window.

NOTE: You must provide the specific group event type from the event list.

Configuring AWS Identity and Access Management

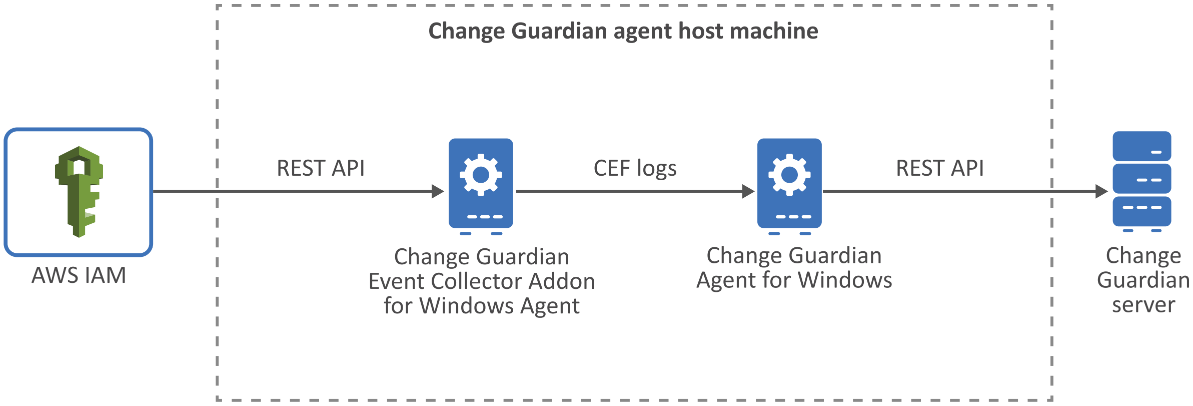
Change Guardian monitors the following in AWS IAM:

- Access Control
- Groups
- Identity and Profiling
- Policies
- User Accounts

This section provides the following information:

- "Implementation Checklist" on page 101
- "Prerequisites" on page 101
- "Configuring Change Guardian for Monitoring" on page 101
- "Categories of Change Guardian Policies for AWS IAM" on page 102

The following diagram illustrates how Change Guardian collects events from AWS IAM:


Change Guardian agent host machine
AWS IAM
REST API
Change Guardian Event Collector Addon for Windows Agent
CEF logs
Change Guardian Agent for Windows
REST API
Change Guardian server

Implementation Checklist

Complete the following tasks to start monitoring AWS IAM events:

Task	See
Complete the prerequisites	"Prerequisites" on page 101
Add the license key	"Adding License for Applications" on page 61
Configure Change Guardian for monitoring	"Configuring Change Guardian for Monitoring" on page 101
	"Categories of Change Guardian Policies for AWS IAM" on page 102
	"Assigning Policies and Policy Sets" on page 126
Triage events	Chapter 8, "Configuring Events," on page 129
	Chapter 9, "Configuring Alerts," on page 135

Prerequisites

Complete the following tasks in the same order:

IMPORTANT: : Install Change Guardian Event Collector Addon for Windows Agent and Change Guardian Agent for Windows on the same machine.

- Install Change Guardian Event Collector Addon for Windows Agent
- Install Change Guardian Agent for Windows
- Install Policy Editor

Configuring Change Guardian for Monitoring

You must configure the Change Guardian server to receive AWS IAM event logs from Change Guardian Event Collector Addon for Windows Agent.

Enabling AWS IAM Monitoring

To enable monitoring:

1. In Agent Manager, select the asset and click **Manage Installations > Install Agents**.

   Or

   In Agent Manager, select the asset and click **Manage Installations > Reconfigure Agents.**
2. In the Reconfigure Agent page, select **Enable Collector Plugin** under **Edit Agent Configuration**.
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** you specify during Change Guardian Event Collector Addon for Windows Agent installation. You can get the CEF data path from the `ceffolder` parameter in `<`*`installation_directory`*`>\current\user\agent\agent.properties`

NOTE: Capturing of events from AWS cloudtrail to CEF logs is delayed. For more information, see Amazon SQS delay queues.

Categories of Change Guardian Policies for AWS IAM

Access Control: Policies about the following:

- Creating and deleting SAML
- Server certificate
- Signing certificate
- Deleting, updating, and uploading SSH
- Enabling, resyncing, and deactivating multi-factor authentication
- Virtual multi-factor authentication

Groups: Polices about creating, changing, and deleting groups

Identity and Profiling: Policies about creating and deleting Instance Profile and OpenID Connect provider

Policies: Policies about the following:

- Attaching and deleting group policy, role policy, and user policy
- Creating and deleting policies and policy versions

User Accounts: Policies about the following:

- Creating, changing and deleting access key, account alias, login profile, role, and user account
- Changing user account password

For information about creating policies in Change Guardian, see "Creating Policies" on page 124.

After creating policies, you can assign them to assets. For information about assigning policies, see "Assigning Policies and Policy Sets" on page 66.

Configuring Office 365 Monitoring

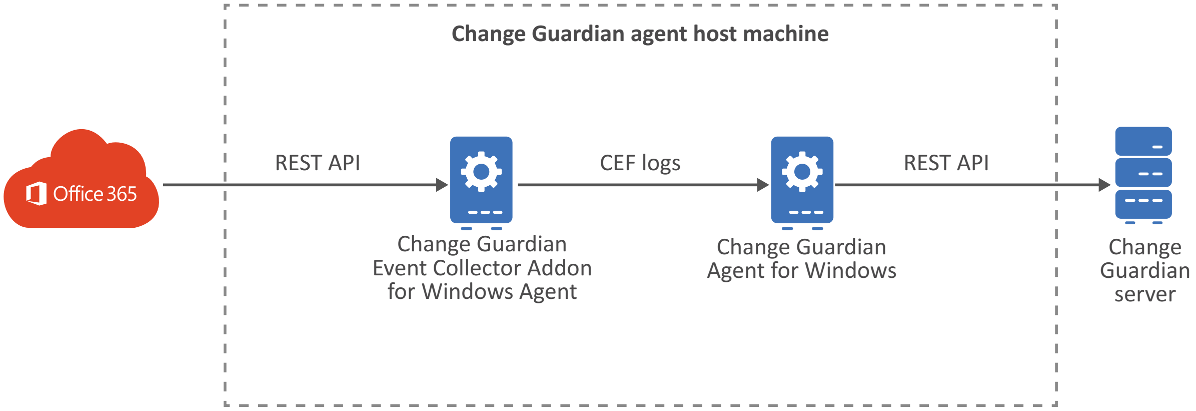
Change Guardian monitors the following in Office 365:

- Exchange Online Settings
- Mailbox Accounts
- Mailbox Messages
- Management Role Groups

This section provides the following information:

- "Implementation Checklist" on page 103
- "Prerequisites" on page 103
- "Configuring Change Guardian for Monitoring" on page 104
- "Categories of Change Guardian Policies for Office 365" on page 104

The following diagram illustrates how Change Guardian collects events from Exchange Online:


Change Guardian agent host machine
Office 365
REST API
Change Guardian Event Collector Addon for Windows Agent
CEF logs
Change Guardian Agent for Windows
REST API
Change Guardian server

Implementation Checklist

Complete the following tasks to start monitoring Office 365 events:

Task	See
Complete the prerequisites	"Prerequisites" on page 103
Add the license key	"Adding License for Applications" on page 61
Configure Change Guardian for monitoring	"Configuring Change Guardian for Monitoring" on page 104
	"Categories of Change Guardian Policies for Office 365" on page 104
	"Assigning Policies and Policy Sets" on page 126
Triage events	Chapter 8, "Configuring Events," on page 129
	Chapter 9, "Configuring Alerts," on page 135

Prerequisites

Complete the following tasks in the same order:

NOTE: IMPORTANT: Install Change Guardian Event Collector Addon for Windows Agent and Change Guardian Agent for Windows on the same machine.

- Install Change Guardian Event Collector Addon for Windows Agent

- Install Change Guardian Agent for Windows
- Install Policy Editor

Configuring Change Guardian for Monitoring

You must configure the Change Guardian server to receive Office 365 event logs from Change Guardian Event Collector Addon for Windows Agent.

Enabling Office 365 Monitoring

To enable monitoring:

1. In Agent Manager, select the asset and click **Manage Installations > Install Agents**.

   Or

   In Agent Manager, select the asset and click **Manage Installations > Reconfigure Agents.**
2. In the Reconfigure Agent page, select **Enable Collector Plugin** under **Edit Agent Configuration**.
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** you specify during Change Guardian Event Collector Addon for Windows Agent installation. You can get the CEF data path from the `ceffolder` parameter in `<`*`installation_directory`*`>\current\user\agent\agent.properties`

Categories of Change Guardian Policies for Office 365

Exchange Online Settings: Policies about creating, deleting, and changing settings, such as role permissions, data loss prevention, anti-malware and retention policies, and mailbox recipients

Mailbox Accounts: Policies about the following:

- Creating and deleting of mailbox accounts
- Enabling and disabling mailbox accounts

Mailbox Messages: Policies about sending on behalf of another user, moving, deleting messages, and so on

Management Roles Groups: Policies about adding, changing, and deleting the following management groups: compliance, discovery, organization, and records

For information about creating policies in Change Guardian, see "Creating Policies" on page 124.

After creating policies, you can assign them to assets. For information about assigning policies, see "Assigning Policies and Policy Sets" on page 66.

Configuring Dell EMC Monitoring

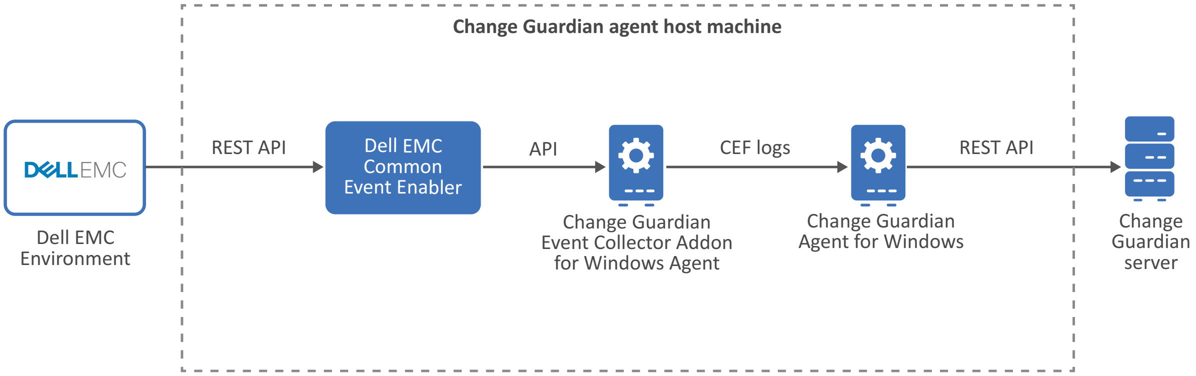
Change Guardian monitors Dell EMC file systems on Isilon and Unity storage platforms.

This section provides the following information:

- "Implementation Checklist" on page 105
- "Prerequisites" on page 106
- "Configuring Change Guardian for Monitoring" on page 106
- "Categories of Change Guardian Policies for Dell EMC" on page 107

The following diagram illustrates how Change Guardian collects events from Dell EMC:

Figure 6-2 *Dell EMC Monitoring using Change Guardian*


Change Guardian agent host machine
DELLEMC
Dell EMC Environment
REST API
Dell EMC Common Event Enabler
API
Change Guardian Event Collector Addon for Windows Agent
CEF logs
Change Guardian Agent for Windows
REST API
Change Guardian server

The deployment diagram illustrates the following:

- Dell EMC Comment Event Enabler (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.
- Change Guardian Event Collector Addon for Windows Agent acts as the interface between Dell EMC and Change Guardian. Change Guardian Event Collector Addon for Windows Agent pulls change 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 start monitoring Dell EMC events:

Task	See
Complete the prerequisites	“Prerequisites” on page 106
Add a license key	“Adding License for Applications” on page 61
Configure Change Guardian for Dell EMC monitoring	“Configuring Change Guardian for Monitoring” on page 106
	“Categories of Change Guardian Policies for Dell EMC” on page 107
	“Assigning Policies and Policy Sets” on page 66
Triage events	Chapter 8, “Configuring Events,” on page 129
	Chapter 9, “Configuring Alerts,” on page 135

Prerequisites

Ensure that you have completed the following:

- Install Change Guardian Event Collector Addon for Windows Agent
- Install Change Guardian Agent for Windows
- Install Policy Editor
- Install Dell EMC CEE, Change Guardian Event Collector Addon for Windows Agent, and Change Guardian Agent for Windows on the same machine

Configuring Change Guardian for Monitoring

You must configure the Change Guardian server to receive Dell EMC event logs from Change Guardian Event Collector Addon for Windows Agent.

Enabling Dell EMC Monitoring

Ensure that you have added Dell EMC assets using Agent Manager.

To enable monitoring:

1 In Agent Manager, select the asset and click **Manage Installations > Install Agents**.

Or

In Agent Manager, select the asset and click **Manage Installations > Reconfigure Agents.**

2 In the Reconfigure Agent page, select **Enable Collector Plugin** under **Edit Agent Configuration**.

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** you specify during Change Guardian Event Collector Addon for Windows Agent installation. You can get the CEF data path from the `ceffolder` parameter in `<`*`installation_directory`*`>\current\user\agent\agent.properties`

NOTE: If the directory name has ".", Dell EMC File Events are not generated.

Categories of Change Guardian Policies for Dell EMC

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

For information about creating policies, see "Creating Policies" on page 124.

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$\ifs\<`*`local sub directory`*`>`
- for Unity, specify `\\onefs8104-1\CHECK$\ifs\<`*`local sub directory`*`>`

Here, `\\onefs8104-1` is the hostname and `\ifs\<`*`local sub directory`*`>` is the directory you want to monitor.

NOTE: You must 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.

After creating policies, you can assign them to assets. For information about assigning policies, see "Assigning Policies and Policy Sets" on page 66.

Configuring Microsoft Exchange Monitoring

Change Guardian monitors the following in Microsoft Exchange:

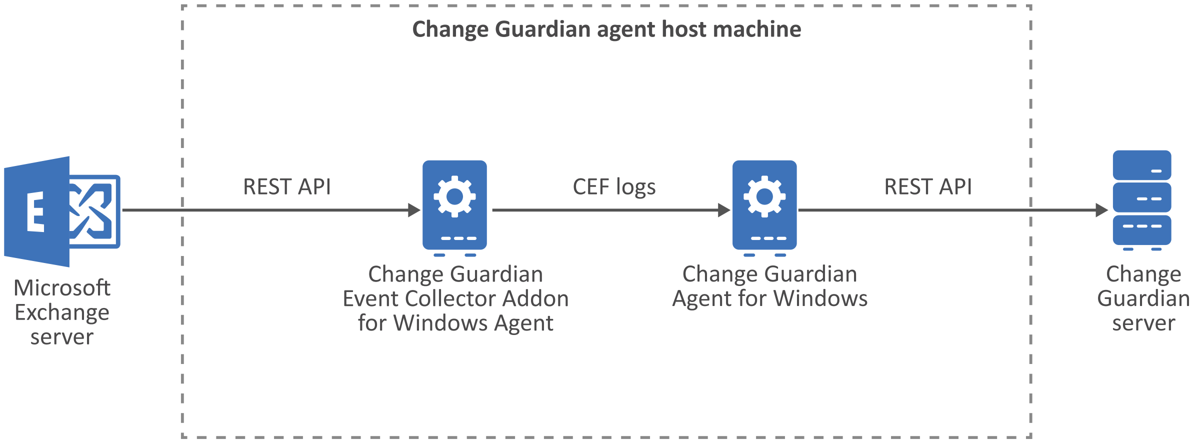
- Exchange Settings
- Mailbox Accounts
- Mailbox Messages
- Management Role Groups

This section provides the following information:

- "Implementation Checklist" on page 108
- "Prerequisites" on page 108
- "Configuring Change Guardian for Monitoring" on page 109
- "Categories of Change Guardian Policies for Microsoft Exchange" on page 110

The following diagram illustrates how Change Guardian collects events from Exchange server:

Figure 6-3 Microsoft Exchange Monitoring using Change Guardian


Change Guardian agent host machine
Microsoft Exchange server
REST API
Change Guardian Event Collector Addon for Windows Agent
CEF logs
Change Guardian Agent for Windows
REST API
Change Guardian server

The deployment diagram illustrates the following:

- Change Guardian Event Collector Addon for Windows Agent acts as the interface between Microsoft Exchange and Change Guardian. Change Guardian Event Collector Addon for Windows Agent pulls change 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

Complete the following the tasks to start monitoring Microsoft Exchange events:

Task	See
Complete the prerequisites	"Prerequisites" on page 108
Add the license key	"Adding License for Applications" on page 61
Configure Change Guardian for monitoring	"Enabling Exchange Monitoring" on page 109 "Categories of Change Guardian Policies for Microsoft Exchange" on page 110 "Assigning Policies and Policy Sets" on page 126
Triage events	Chapter 8, "Configuring Events," on page 129 Chapter 9, "Configuring Alerts," on page 135

Prerequisites

Complete the following tasks in the same order:

IMPORTANT: Install Change Guardian Event Collector Addon for Windows Agent and Change Guardian Agent for Windows on the same machine as Microsoft Exchange server.

1. Install Change Guardian Event Collector Addon for Windows Agent
2. Install Change Guardian Agent for Windows
3. Install Policy Editor

Configuring Change Guardian for Monitoring

You must configure the Change Guardian server to receive Exchange event logs from Change Guardian Event Collector Addon for Windows Agent.

Enabling Exchange Monitoring

Ensure that you have added Exchange assets in Agent Manager.

To enable monitoring:

1. In Agent Manager, select the asset and click **Manage Installations > Install Agents**.

   Or

   In Agent Manager, select the asset and click **Manage Installations > Reconfigure Agents.**
2. In the Reconfigure Agent page, select **Enable Collector Plugin** under **Edit Agent Configuration**.
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** you specify during Change Guardian Event Collector Addon for Windows Agent installation. You can get the CEF data path from the `ceffolder` parameter in `<`*`installation_directory`*`>\current\user\agent\agent.properties`.

Adding Exchange Mailbox Alias

To receive mailbox events, add the Exchange mailbox alias in Change Guardian Event Collector Addon for Windows Agent.

To add:

1. Launch Change Guardian Event Collector Addon for Windows Agent.
2. Under **Select the collector to configure**, click **Modify** next to **Exchange**.
3. Click **Next**.
4. On **What would you like to do? screen**, click **Modify Connector > Next**.
5. On **What would you like to do with the connector?** screen, click **Modify connector parameters > Next**.
6. On **Modify table parameters** screen, add the alias name as a new row.
7. On **Would you like to continue or exit?** screen, click **Exit**.
8. Open Windows Services and restart the **ArcSight Microsoft Exchange PowerShell** service.

Categories of Change Guardian Policies for Microsoft Exchange

Exchange Settings: Policies about creating and deleting configuration settings

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

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

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

For information about creating policies, see "Creating Policies" on page 124.

After creating policies, you can assign them to assets. For information about assigning policies, see "Assigning Policies and Policy Sets" on page 66.

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

Configuring NetApp Storage Monitoring

Storage solutions such as NetApp store a large amount of data and, therefore, can have a large volume of audit events. 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 from the audit scope to ensure a faster and more efficient audit process.

Change Guardian monitors file systems in NetApp, and supports both Common Internet File System (CIFS) and Network File System (NFS) protocols.

- "Implementation Checklist" on page 110
- "Prerequisites" on page 111
- "Configuring Change Guardian for Monitoring" on page 114
- "Categories of Change Guardian Policies for NetApp" on page 115

Implementation Checklist

Complete the following tasks to start monitoring NetApp events:

Task	See
Complete the prerequisites	"Prerequisites" on page 111
Add a license key	"Adding License for Applications" on page 61
Configure Change Guardian for monitoring	"Categories of Change Guardian Policies for NetApp" on page 115 "Assigning Policies and Policy Sets" on page 126

Task	See
Triage events	Chapter 8, “Configuring Events,” on page 129 Chapter 9, “Configuring Alerts,” on page 135

Prerequisites

Ensure that you have completed the following:

- Install a supported version of Data ONTAP Cluster Mode
- Install Change Guardian Agent for UNIX

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

- Install Policy Editor
- Configure NetApp

Configuring the NetApp Native Auditing

Configure the NetApp native auditing solution to monitor file and directory events on your Storage Virtual Machines (SVM) with a FlexVol volume.

NOTE: Change Guardian documentation provides the third-party configuration steps for ease of use. For more information about the third-party products or for any issues with the configuration, see their documentation.

The security descriptor may contain Discretionary Access Control Lists (DACLs) to apply to file and folder access permissions. On the other hand, the security descriptor may contain System Access Control Lists (SACLs) for file and folder auditing, or even both SACLs and DACLs.

For better performance, store the audit file in a separate volume and mount the complete share on the agent machine.

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

Configure NetApp auditing depending on the filesystem it uses:

- “Configuring NetApp Native Auditing for CIFS” on page 112
- “Configuring NetApp Native Auditing for NFS” on page 112

NOTE: Ensure that you have the root user privilege to complete these tasks.

Configuring NetApp Native Auditing for CIFS

Create an auditing configuration on the given SVM for CIFS before you can monitor events on NetApp storage. You can monitor these events on CIFS by setting SACLs 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:

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

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

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

3. Set NTFS audit policies using the Windows Security tab.

   For information about the steps, see *Apply a basic audit policy on a file or folder* in the Microsoft Documentation site.

4. Verify audit configuration:

   ```
   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, 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
   ```

5. Enable SVM auditing:

   ```
   vserver audit enable -vserver <Name_SVM>
   ```

   Example:

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

Configuring NetApp Native Auditing for NFS

To configure auditing in NFS:

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

```
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 is `audit`, then the command is:

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

3 Verify audit configuration:

```
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 To configure Change Guardian Agent for UNIX to monitor the NetApp filesystem changes, enable ACL for NFS:

```
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
```

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

5a Run the `mkdir <Folder_Name>` command to create a mount directory.

5b Mount to the directory:

```
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
```

5c To monitor each folder within a volume, add audit flags recursively on each folder in the mount directory you want 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
```

5d To monitor an entire volume, add audit flags recursively on the mount directory that 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
```

6. Enable SVM auditing:

   ```
   vserver audit enable -vserver <Name_SVM>
   ```

   Example:

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

Configuring Change Guardian for Monitoring

After configuring NetApp audit, mount the NetApp volumes into Change Guardian Agent for UNIX. Mount one volume for audit logs and another for CIFS or NFS shares to monitor.

Complete the following tasks to configure Change Guardian:

- "Mounting the Audit Logs in CIFS" on page 114
- "Mounting the Audit Logs in NFS" on page 115
- "Creating a Configuration File" on page 115

NOTE: Ensure that you have the required permission to complete these tasks. Check with your network or system administrator for assistance.

Mounting the Audit Logs in CIFS

To mount the audit log:

1. Create a mount directory.

   Example:

   ```
   mkdir /mnt/audit
   ```

2. Go to `/usr/netiq/vsau/etc` and create a file `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 its credentials:

   ```
   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/audit /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 for the audit file.

Mounting the Audit Logs in NFS

Create a mount point in the Change Guardian 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: Make changes to `/etc/fstab` and mount the volume with the NetApp share following the above steps.

Creating a Configuration File

Complete the following steps in the Change Guardian Agent for UNIX machine:

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 follows:

```
x.x.x.x,/vol1,/mnt/audit,vol1
```

Categories of Change Guardian Policies for NetApp

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

NOTE: Specify the `/folder_name` 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 about creating policies, see "Creating Policies" on page 124.

After creating policies, you can assign them to assets. For information about assigning policies, see "Assigning Policies and Policy Sets" on page 66.

Configuring Linux or UNIX Monitoring

Change Guardian monitors the following in Linux and UNIX environments:

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

This section provides the following information:

- "Implementation Checklist" on page 116
- "Prerequisites" on page 117
- "Categories of Change Guardian Policies for UNIX" on page 122

Implementation Checklist

Complete the following tasks to start monitoring Linux and UNIX events:

Task	See
Complete the prerequisites	"Prerequisites" on page 117
Add a license key	"Adding License for Applications" on page 61
Configure Change Guardian for monitoring	"Categories of Change Guardian Policies for UNIX" on page 122
	"Assigning Policies and Policy Sets" on page 126
Triage events	Chapter 8, "Configuring Events," on page 129
	Chapter 9, "Configuring Alerts," on page 135

Prerequisites

Ensure that you have completed the following:

- Install Change Guardian Agent for UNIX
- Install Policy Editor
- Configure Auditing in UNIX or Linux

Configuring Auditing in UNIX or Linux

You must enable the auditing system of your UNIX or LINUX operating systems to allow Change Guardian to start monitoring.

NOTE: Change Guardian documentation provides the third-party configuration steps for ease of use. For more information about the third-party products or for any issues with the configuration, see their documentation.

- "Configuring a UNIX Auditing Subsystem" on page 117
- "Configuring a Linux Auditing Subsystem" on page 121

NOTE: Ensure that you have the root user privilege to complete these tasks.

Configuring a UNIX Auditing Subsystem

This section provides information about configuring auditing on UNIX computers:

- "Configuring the AIX Audit Subsystem" on page 117
- "Configuring the HP-UX Audit Subsystem" on page 120
- "Configuring the Solaris Auditing Subsystem" on page 120

Configuring the AIX Audit Subsystem

Auditing subsystem stores files in the `/etc/security/audit` folder. However, in AIX computers, streaming all events might consume too much memory or processor time and enable only the minimum required auditing.

You can enable AIX audit subsystem either in `STREAM` or `BIN` mode.

To configure AIX audit subsystem:

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

```
start:
```

```
bin:
     trail = /audit/trail
     bin1 = /audit/bin1
     bin2 = /audit/bin2
     binsize = 10240
  cmds = /etc/security/audit/bincmds
stream:
  cmds = /etc/security/audit/streamcmds
classes:
     general =
USER_SU,PASSWORD_Change,FILE_Unlink,FILE_Link,FILE_Rename,FS_Chdir,FS_
Fchdir,FS_Chroot,PORT_Locked,PORT_Change,FS_Mkdir,FS_Rmdir,FILE_Symlin
k,USER_Exit,PROC_Create,PROC_Delete,FILE_Fchmod,FS_Rmdir,GROUP_User,GR
OUP_Adms,GROUP_Change,GROUP_Create,GROUP_Remove,USER_Remove,USER_Creat
e,USER_Chpass,USER_Change,FS_Mount,FS_Umount,FILE_Unlinkat,FILE_Symlin
kat
     Kernel =
PROC_Create,PROC_Delete,PROC_Execute,PROC_RealUID,PROC_AuditID,PROC_Re
alGID,PROC_Environ,PROC_SetSignal,PROC_Limits,PROC_SetPri,PROC_Setpri,
PROC_Privilege,PROC_Settimer,PROC_LPExecute,PROC_Adjtime,PROC_Kill
     files =
FILE_Open,FILE_Read,FILE_Write,FILE_Close,FILE_Link,FILE_Unlink,FILE_R
ename,FILE_Owner,FILE_Mode,FILE_Acl,FILE_Privilege,DEV_Create,FILE_Dup
fd,FILE_Chmod,FILE_Chown,FILE_Utimes,FILE_Truncate,FILE_Mknod,FILE_Sym
link,FILE_Unlinkat,FILE_Fchownat,FILE_Linkat,FILE_Fchown,FILE_Symlinka
t,FILE_Openxat,FILE_Mknodat,FILE_Renameat,FILE_Fchownat,FILE_Fchmod,FI
LE_Fchown,FILE_Fchmodat
     cron =
AT_JobAdd,AT_JobRemove,CRON_JobAdd,CRON_JobRemove,CRON_Start,CRON_Fini
sh
users:
     root = general,Kernel,files,cron
     default = general,Kernel,files,cron
role:
```

2 (Conditional) To enable `STREAM` mode, perform the following steps:

2a Add the following to `/etc/security/audit/config` file:

```
start:

     binmode = off

     streammode = on
```

2a1 Add the following line to the`/etc/security/audit/streamcmds` file:

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

3 (Conditional) To enable `BIN` mode, perform the following steps:

3a Disable stream mode and enable bin mode in the `/etc/security/audit/config` file

3b Add the following line to`/etc/security/audit/bincmds` file:

```
/usr/sbin/auditcat $bin | /usr/sbin/auditpr -t 0 -r -v -helRtcrpPTh
>> /audit/trail
```

3c Add the following line to/etc/security/audit/streamcmds file:

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

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

- FS_Mount
- FILE_Unlinkat
- CRON_Finish
- FILE_Linkat
- CRON_JobRemove
- PROC_Kill
- PROC_Execute
- FILE_Unlink
- FILE_Rename
- FILE_Fchown
- FILE_Owner
- USER_Chpass
- FILE_Symlinkat
- USER_Change
- FILE_Symlink
- PROC_LPExecute
- FILE_Open
- FILE_Mknodat
- FILE_Dupfd
- FILE_Chmod
- FILE_Renameat
- USER_Create
- GROUP_Create
- FS_Chdir
- FS_Umount
- FILE_Chown
- FILE_Fchownat
- GROUP_Change
- PROC_Create
- USER_Remove
- FILE_Fchmod
- PROC_Adjtime
- CRON_JobAdd
- FILE_Utimes

- PROC_Delete
- FILE_Openxat
- GROUP_Remove
- FILE_Fchmodat
- FILE_Mode
- PROC_Settimer
- FILE_Mknod
- CRON_Start
- FILE_Link

5. Restart the audit subsystem.
6. Restart `detectd` service from the given location:

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

Configuring the HP-UX Audit Subsystem

The auditing subsystem on HP computers stores files in the `/etc/rc.config.d` directory. Ensure that the `/etc/rc.config.d/auditing` file includes the following lines:

```
AUDITING=1

PRI_AUDFILE=/.secure/etc/audfile1

PRI_SWITCH=1000

SEC_AUDFILE=/.secure/etc/audfile2

SEC_SWITCH=1000

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

AUDEVENT_ARGS2=" "
AUDEVENT_ARGS3=" "
AUDEVENT_ARGS4=" "
AUDOMON_ARGS=" -p 20 -t 1 -w 90"
```

Configuring the Solaris Auditing Subsystem

To configure on Solaris 10:

1. To ensure that the Basic Security Module restarts after reboot, run the following command from the `/etc/security` folder.

   ```
   ./bsmconv
   ```

2 Ensure that the `/etc/security/audit_control` file contains the following lines:

```
flags: ua,fm,pc,fw,fr,ad,as,fc,ps,fd,nf
naflags: fm,pc,fw,fr,as,ad,fc,ps,fd,nf
minfree:20
dir:/var/audit
```

To configure on Solaris 11:

1 Set the auditing flags as follows:

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

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

Configuring a Linux Auditing Subsystem

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

To configure:

1 (Conditional) For RHEL, ensure that the `auditd` service is enabled:

```
chkconfig auditd on
```

2 (Conditional) For SUSE, perform the following steps:

2a Check if the audit process is running:

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

2b If the audit process is running in disabled mode, enable the process:

`/sbin/auditd -s enable`.

2c Ensure that the PID in the command output matches the PID of the enabled process:

```
auditctl -e 1
```

2d To enable syscall auditing:

Comment out the line `-a task,never` from the below file:

`/etc/audit/rules.d/audit.rules`. Restart the audit service.

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

Converting Agent from Non-FIPS to FIPS mode

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

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

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

Categories of Change Guardian Policies for UNIX

Configuration Files: Policies about changing hostname resolution and process startup configuration

CRON: Policies to monitor accessing CRON job, and changing CROS task execution

Exported File System: Policies to monitor list of exported file system

File Integrity: Policies to monitor Change Guardian 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 built-in users

For information about creating policies, see "Creating Policies" on page 124.

After creating policies, you can assign them to assets. For information about assigning policies, see "Assigning Policies and Policy Sets" on page 66.

7 Configuring Change Guardian Policies

Policies allow you to define how Change Guardian monitors assets in your environment. A policy includes one or more criteria to define a specific change event you want to monitor in your enterprise. Change Guardian collects events based on the Change Guardian policies. This chapter provides an overview about policies, information about how to create policies and policy sets, assign event designations to a policy, and so on.

Understanding Policies and Policy Sets

Policies allow you to identify the asset you are monitoring, and then add any combination of the following criteria:

- Add filters to narrow the monitoring target and results
- Define managed users for the activity
- Assign event contexts to categorize policies
- Specify a custom severity that matches the policy

Each Change Guardian application includes several policy types.

You must apply a policy to an agent that is collecting events from the asset. You can combine multiple policies from one or more agents to organize and manage monitoring the agents. You can include a policy in multiple policy sets.

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 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 is successful.

NOTE: Change Guardian automatically calculates Event Severity for Change Guardian Agent for UNIX events, including events generated by policies configured with a custom severity.

Examples of severity are as follows:

- **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: Change Guardian allows managed users to make specific changes to assets. When managed users make changes, the generated events appear as managed change events. When creating or editing a policy, use the **Managed Events** to specify the managed users for the policy.

If you specified a user group as a managed user, and the group membership changes, Change Guardian synchronizes associated policies with the new group members.

Event Context: Use the Event Context section to categorize the policy and specify its purpose. Generated events include the event contexts. You can create new event contexts with user-defined values. You can select one or more of the following default event contexts:

- Risk Domain
- Risk
- Sensitivity
- Regulation/Policy
- Control/Classification
- Response Window

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 that each user of the Group A performs. If the policy returns an event, the name of the user performing the change is included in the event report.

Configure LDAP server for every grouped resource. You can either add the Active Directory items manually or browse them while creating a policy. A policy cannot monitor the group members correctly if you only specify the grouped resource in a policy, but do not configure LDAP settings for the grouped resource.

Creating Policies

You can create a policy by using one of the following methods:

- Create a fresh policy with no preconfigured settings
- Clone and customize a template

Creating a Fresh Policy

You can create a fresh policy without preconfigured settings.

To create a policy:

1. In Policy Editor, select one of the applications, such as Active Directory.
2. Expand the list of policies and select the policy type you want to create. For example, select **Active Directory Policies > AD Object**.

3 On the Configuration Policy screen, make the appropriate changes.

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

NOTE: For more information about enabling a policy, see "Enabling a Change Guardian Policy Revision" on page 126.

Working with Policies

Change Guardian stores the policies in the Change Guardian policy repository.

After creating a policy, you can perform various activities such as clone a policy, assign the policy to an agent, and schedule policy monitoring. While working with policies, ensure that you follow the order specified below:

1. Submit a policy or make the policy available by cloning from a template
2. Enable the policy

This section provides the following information:

- "Cloning a Change Guardian Policy" on page 125
- "Creating Change Guardian Policy Sets" on page 126
- "Assigning Policies and Policy Sets" on page 126
- "Enabling a Change Guardian Policy Revision" on page 126
- "Exporting and Importing Change Guardian Policies" on page 126
- "Assigning Event Destinations to Change Guardian Policies" on page 127
- "Scheduling Change Guardian Policy Monitoring" on page 127

Cloning a Change Guardian Policy

Cloning a policy allows you to create a policy based on an existing policy and then make changes as required. By default, Change Guardian uses the latest revision of the selected policy when creating a clone. You can also select a specific policy revision.

Cloning a Template

Policy templates provide examples of best configured policies that you can reuse. Applying a policy template from the platform template library clones the policy into your active policy area. Edit the criteria to specify the agent and files to be monitored.

To clone from a template:

1 In Policy Editor, under the desired application, select the template you want to apply.

2 Specify the required information, and click **Submit**.

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

NOTE: For more information about enabling a policy, see "Enabling a Change Guardian Policy Revision" on page 126.

Creating Change Guardian Policy Sets

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

Use the Policy Set Manager to add, edit, or clone policy sets. To open Policy Set Manager, click **Change Guardian > Policy Set Manager**.

Assigning Policies and Policy Sets

For information about assigning policies and policy sets, see "Assigning Policies and Policy Sets" on page 66.

Enabling a Change Guardian Policy Revision

When you change a policy, Change Guardian creates a new revision of that policy. Policy revisions allow you to keep and share work that is in progress. You can view all policy revisions and the version number of the currently enabled policy in Policy Editor. You can edit and enable a previous revision of a policy.

To enable an older revision:

1. Select the desired policy under the application name.
2. On the **History** tab, enable the required policy revision.
3. Assign the policy.

NOTE: If you update the revision of a policy that is already assigned, Change Guardian automatically updates all associated agents with the new revision of that policy.

Exporting and Importing Change Guardian Policies

Change Guardian allows you to export a policy to a `.xml` file. You can import that policy as a new policy. You can also modify an imported policy to create a new policy with a similar definition. You can export one policy at a time, however, you can import multiple policies at a time.

To export a policy:

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

To import a policy:

1. In Policy Editor, 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. You can use the new event destination along with the default event destination or replace it. The updated event destination takes effect when the agent receives the updated policy information at the next heartbeat.

To assign:

1. In Policy Editor, click **Change Guardian > Policy Assignment**.
2. Select an asset or asset group, and click **Assign Policies**.
3. Select a policy set or policy, and click **Advanced**.
4. Select one or more event destinations to assign to the specified policy or policy set.

For information about creating event destinations, see "Creating Event Destinations" on page 130.

Scheduling Change Guardian Policy Monitoring

Change Guardian policies monitor agents and agent groups continuously. A monitoring schedule allows you to define specific times at which a policy or policy set monitors agents and agent 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 agent or agent group, you can attach a monitoring schedule.

To create a monitoring schedule, in Policy Editor, click **Settings > Schedule Monitoring Time**. You can set the following schedule during which you want to suspend monitoring: Mondays from 3-5 p.m. and Tuesdays from 4-6 p.m.

8 Configuring Events

Change Guardian collects events from various assets based on pre-configured Change Guardian policies. Events are collected by Change Guardian agents and are received by the Change Guardian server and displayed in the Events dashboard. To view events, log in to the Change Guardian web console.

By default, events are stored in the server temporarily, based on the data retention value. However, you can choose to store all or specified event data to a syslog server or in another Change Guardian server or a Sentinel server.

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 131.

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 138.

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" on page 130
- "Assigning Event Destinations" on page 131

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 web console, click **CONFIGURATION > Events > Event Destinations**.
2. Click **Add**.
3. Specify a unique name for the event destination.
4. Specify one of the event destination models.
5. 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 agents, 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.

6. (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.

7. 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 agents, 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 agent reads the updated policy information.

To assign:

1. Log in to the web console, click **CONFIGURATION > Policies > Assign Policies**
2. Select **Agents** or **Agent Groups** and click the edit icon under **Assign Unassign** option.
3. Select a policy set or policies to enable the **Event Destinations** option.
4. Once it is enabled, click **Event Destinations**.
5. Select a policy from the drop-down list and assign one or more event destinations.
6. Click **SAVE** and **APPLY**.

NOTE: Policies that are a part of a policy set are not shown in the *Policies* tab. They are available under *Policy Sets* and contain the properties of the set. If the set is assigned with additional destination, it reflects after an upgrade. If the policy is assigned with an additional destination before moving to the set, it is not retained post upgrade. Since the policy is no longer available under *Policies*, it cannot be assigned separately to any destination.

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 132
- "Ordering Event Routing Rules" on page 132
- "Activating or Deactivating an Event Routing Rule" on page 132

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. For information about creating event routing rules, see "Creating Event Routing Rules" on page 67.

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 location. 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 the web console, click **ADMINISTRATION > 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 the web console, click **ADMINISTRATION > 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*.

9 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.

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 Alert Dashboard.

   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.

NOTE: When you create Office 365 and Exchange alerts based on event names, include the following policy definitions: " includes events only when event name matches Exchange server/... " and "includes events only when generated by policies *policies*". This ensures that you receive separate events for Office 365 and Exchange. If you do not add the conditions in the policy definition, Change Guardian might raise two alerts for the same event, because user operations are common in Office 365 and Exchange.

This section provides the following information:

- "Creating Alert Rules" on page 136
- "Redeploying Alert Rules" on page 137
- "Configuring Event Destinations to Generate Alerts" on page 138

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.

Configuring Event Destinations to Generate Alerts

To ensure alert rules generate alerts on the alternate event destinations when both the default and the alternate event destinations are 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.

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 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

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. From the web console, click **ADMINISTRATION > Routing > Alert Routing Rules > Create**.
2. 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.
3. Specify whether you want to enable the alert routing rule at this time.
4. 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

You can use the following consoles to analyze alerts:

- "Threat Response Dashboard" on page 139
- "Alerts View" on page 140
- "Alert Dashboard" on page 140

Threat Response Dashboard

The Threat Response dashboard provides an overview of alerts generated by the Change Guardian server.

You can perform the following operations on this dashboard:

- View alerts in new state by ownership and priority

- Customize the default view to display alerts in investigating state
- View the list of alerts and their details

Alerts View

The alerts you can view depend on the alert permissions applicable to your role and the tenancy of your role. For more information about permission to manage alerts, see "Understanding the Roles" on page 68.

Using the Alerts View you can perform the following operations:

- Assign alerts to other users
- Change the state of an alert to New, Investigating, or Closed

  If you do not manually close an alert, it remains open.
- Export alerts to an Excel file
- Share content with others using a URL
- View alert details such as the event that triggered the alert, the rule that generated the alert, the list of users involved in the alert, and so on

NOTE: The alert retention policies control when the alerts should be closed and deleted from Change Guardian. For information about configuring alert retention policies, see "Configuring Alert Retention Policies" on page 140.

Alert Dashboard

You can see a high-level overview of the alerts in your organization using the Alert dashboard. Using the Alert dashboard you can analyze and study common patterns in alerts. A Change Guardian `admin` can investigate alerts, monitor team load, and monitor performance against tenant service-level agreement (SLA).

- Types of alerts
- Average time taken to close alerts
- Top correlation rule generating the maximum number of alerts
- Geographical origin of high-severity alerts
- Oldest open alerts
- Alerts that took the longest time to close

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. 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. From the web console, click **ADMINISTRATION > Storage > Alert**.
2. 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.
3. Save the alert retention policy.

Viewing Federated Alerts

To view alerts in a distributed environment, log in to the authorized requestor server as a user with `Search Remote Data Sources` permission, select the data source servers from which you want to view alerts while creating alert views.

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.

Understanding Data Federation

When data federation is enabled, you can perform a search or run a report on 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, the following happens:

- Search queries are sent to each selected data source server
- Data source server authenticates the authorized requestor server
- Event or alert data is returned to the authorized requestor, where it is merged, sorted, and rolled up for presentation
- The search status for each data source server is displayed.

  Search results contain information about data source servers from which they originated.

Configuring an Authorized Requestor for Data Federation

You must first enable data federation on the authorized requestor server and then add data source servers to the authorized requestor server. You can add data source servers in the following ways:

- If you know the administrator username and password for the data source server, add the data source server directly from the authorized requestor.
- If you do not know the administrator username and password for a data source server, set up the authorized requestor with an opt-in password and share it with the source server. The administrator can use the opt-in password to add the data source servers to the authorized requestor.

To generate a report about the health of agents on federated servers, see “Agent Health on Federated Servers” in the *Change Guardian Online Help*.

- “Enabling Data Federation” on page 144
- “Using the Administrator Credentials to Add a Data Source Server” on page 145
- “Using the Opt-in Password to Add a Data Source Server” on page 146

For troubleshooting tips, see “Issues on Federated Servers” on page 238.

Enabling Data Federation

To enable:

1. Create a role with **Proxy for Authorized Data Requestors** permission in the data source server.

   For more information about configuring users and roles, see Configuring Roles and Users.
2. On your requestor machine, click **Administration > Integration > Change Guardian**.
3. In the **Data Sources** section, select **Local server and other data sources**.
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 username and password for the data source server, continue with “Using the Administrator Credentials to Add a Data Source Server” on page 145.
   - 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, continue with “Using the Opt-in Password to Add a Data Source Server” on page 146.

Configuring Data Federation in FIPS Mode

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

Adding Certificates

To add:

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

   ```
   cd /etc/opt/novell/sentinel/config/
   ```
3. Copy the source certificate (`sentinel.cer`) to a temporary location on the requestor computer.
4. Import the source certificate into the FIPS keystore of the requestor server.

   For more information about importing the certificate, see Importing certificates into the FIPS keystore database.
5. Log in to the distributed search requestor computer.
6. Browse to the following certificate directory:

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

7 Copy the requestor certificate (`sentinel.cer`) to a temporary location on the source computer.

8 Import the requestor system certificate into the FIPS keystore of the source server.

For more information about importing the certificate, see Importing certificates into the FIPS keystore database.

Importing Certificates

To import:

1 Copy the certificate file to any temporary location on the Change Guardian server or remote Collector Manager.

2 Change the ownership of the certificate to `novell` user:

```
chown novell:novell /<path to certificate>
```

3 Change the permission of the certificate:

```
chmod 644 /<path to certificate>
```

4 Switch to `novell` user.

5 Browse to the Sentinel bin directory.

The default location is `/opt/novell/sentinel/bin`.

6 Import the certificate into the FIPS keystore database, and then follow the on-screen instructions:

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

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

Using the Administrator Credentials to Add a Data Source Server

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

IMPORTANT: Ensure that the data source server that you add is able to communicate with the authorized requestor through TCP/IP. Use a ping command to ensure that the IP address or hostname of the data source server is accessible through firewalls or NATs. If there is a communication failure, an error is displayed in the extended status page. For more information, see "“Managing Search Results” on page 193”

To add a data source server:

1 Complete the steps in “Enabling Data Federation” on page 144.

2 Click the **Add a data source** link.

3 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: Name of a user with administrator privileges.

Password: Password associated with the username.

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

5 Specify the following information to configure the data source server:

Name: Specify a descriptive name to identify the data source server.

Search Proxy Role: Select a search proxy role that you want to assign to the authorized requestor. This permission is required for the data source server to accept and process incoming search requests from the authorized requestor server.

When the authorized requestor makes search requests to the data source server, the security filter of the proxy role is used. Only those events that pass the security filter of the proxy role 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.

6 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, Running Reports in a Federated Setup, and Viewing Federated Alerts respectively.

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

In organizations where administrative control of Change Guardian servers is decentralized, sharing administrator password might lead to violation of the security policy. If you do not have the administrator password for the data source server, Change Guardian allows you to 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.

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.

When a data source server opts in to the authorized requestor, a message is sent to the authorized requestor server requesting to be added to the list of data source servers. The authorized requestor requires an opt-in password to verify that the opt-in request has originated from a valid data source server. The request authorizes the authorized requestor to access data on the data source server.

- “Setting the Opt-In Password” on page 146
- “Allowing Access to an Authorized Requestor Server” on page 147

Setting the Opt-In Password

To set the password:

1 Complete the steps in “Enabling Data Federation” on page 144.

2 Click **Integration > Change Guardian**.

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 "Allowing Access to an Authorized Requestor Server" on page 147 to add the data source server to the authorized requestor.

Allowing Access to an Authorized Requestor Server

To allow access:

1 Log in to the data source server as an administrator.

2 Click **Integration > Change Guardian**.

3 From the **Authorized Requestors** section, check the **Allow authorized requestors to access data from your server** box.

4 Click the **Add** link.

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**.

7 Verify the certificate information, then click **Accept**.

8 Specify the following information to configure the data source server:

Name : A descriptive name to identify the authorized requestor server.

Search Proxy Role : A proxy role to assign to the authorized requestor.

This permission is required for the data source server to accept and process incoming search requests from the authorized requestor server. When the authorized requestor makes search requests to the data source server, the security filter of the proxy role is used. Only those events that pass the security filter of the proxy role are returned to the authorized requestor server. Only roles that have the Proxy for Authorized Requestors permission are listed.

9 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.

Viewing Search Activities

You can view the type and frequency of search activities run on the data source server by the authorized requestor server. Based on the search activity, you might want to assign a more or 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 the queries performed today, yesterday, or in the last hour. You can also see the queries that were made by particular users on the authorized requestor.

To view search:

1 Log in to the data source server as an administrator.

2 Click **Integration > Change Guardian**.

3 From the **Authorized Requestors** section, click the **Search Activities** link for the authorized requestor server for which you want to view the search activities.

   A list of the audit events that are retrieved from all the distributed search requests that a data source server has received from an authorized requestor are displayed.

Modifying the Data Source Server Details

You can modify the name of the data source server and the port number.

To modify the details:

1 From the web console, click **ADMINISTRATION > Integration > Change Guardian**

2 In the **Data Sources** section, click the **Edit** link for the data source server that you want to modify.

3 Make the necessary modifications.

4 (Optional) To change the proxy role on the data source server, complete the following steps:

   4a Click **View/Change**.

   4b Log in to the data source server.

   4c Select a proxy role, then click **OK**.

5 Click **Save**.

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, and track Active Directory using Directory and Resource Administrator (DRA) as events.

This chapter provides the following information:

- "Integration with SIEM Solutions" on page 149
- "Integrating with Identity Management Solutions" on page 149
- "Integration with Directory Resource Administrator" on page 151

Integration with SIEM Solutions

Change Guardian and the SIEM solution products, such as Micro Focus Sentinel Enterprise, Splunk Enterprise Security, and Micro Focus Security ArcSight Logger 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
Micro Focus Security ArcSight Logger	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 129.

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

Integrating AD with Change Guardian provides user information from AD and user mapping with associated incoming events. For more information, see "Configuring LDAP for AD Browsing" on page 62.

To view identity information and view the recent activities of a user, see Viewing Identity Data.

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.

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. You can view events by clicking ADMINISTRATION from the web 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.

Prerequisites:

Ensure that you have completed the following:

- Install DRA
- Install Change Guardian

Setting Up Change Guardian

To set up Change Guardian to receive DRA events, perform the following steps:

- Installing Change Guardian Agent for Windows
- Configuring AD
- Creating an AD Policy
- Assigning Policies

Setting Up DRA

To set up DRA, perform the following steps:

- To “manage AD domains”, see the *Directory and Resource Administrator Administration Guide*
- Enabling Event Stamping
- Configuring Unified Change History

Enabling Event Stamping in DRA

Event stamping allows Change Guardian to receive the DRA user details.

When AD Domain Services auditing is enabled, DRA events are logged as having been generated by either the DRA Service account or the Domain Access account if one is configured. Event Stamping takes this feature one step further by generating an additional AD DS event that identifies the assistant administrator who performed the operation.

For these events to be generated you must configure AD DS auditing and enable Event Stamping on the DRA Administration Server. When Event Stamping is enabled, you will be able to view the changes that assistant administrators make in Change Guardian Event reports.

- To configure AD DS auditing, see the Microsoft reference *AD DS Auditing Step-by-Step Guide*.
- To configure Change Guardian integration, see “Configuring Unified Change History Servers” on page 152.

- To enable Event Stamping, open the Delegation and Configuration console as DRA Administrator, and do the following:
  1. Navigate to **Configuration Management** > **Update Administration Server Options** > **Event Stamping**.
  2. Select an object type, and click **Update**.
  3. Select an attribute to use for Event Stamping for that object type.

     DRA currently supports Event Stamping for users, groups, contacts, computers, and organizational units.

     DRA also requires that the attributes exist in the AD schema for each of your managed domains. You should be aware of this if you add managed domains after configuring Event Stamping. If you were to add a managed domain that does not contain a selected attribute, operations from that domain would not be audited with the Event Stamping data.

     DRA will be modifying these attributes so you should select attributes that are not used by DRA or any other application in your environment.

Configuring Unified Change History in DRA

The Unified Change History Server feature enables you to generate reports for changes made outside of DRA.

Delegating the Unified Change History Server Configuration Powers

To manage Unified Change History Server, assign the Unified Change History Server Administration role or the applicable powers below to assistant administrators:

- Delete Unified Change History Server Configuration
- Set Unified Change History Configuration Information
- View Unified Change History Configuration Information

To delegate Unified Change History Server powers:

1. Click **Powers** in the Delegation Management node, and use the search objects feature to find and select the UCH powers that you want.
2. Right-click one of the selected UCH powers and select **Delegate Roles and Powers**.
3. Search for the specific user, group, or assistant administrator group that you want to delegate powers to.
4. Use the **Object Selector** to find and add the objects that you want, and then click **Roles and Powers** in the **Wizard**.
5. Click **ActiveViews**, and use the **Object Selector** to find and add the ActiveViews that you want.
6. Click **Next** and then **Finish** to complete the delegation process.

Configuring Unified Change History Servers

To configure Unified Change History Servers:

1. Log in to the Delegation and Configuration Console.
2. Expand **Configuration Management** > **Integration Servers**.

3. Right-click **Unified Change History**, and select **New Unified Change History Server**.
4. Specify the UCH server name or IP address, port number, server type, and access account details in the Unified Change History configuration.
5. Test the server connection and click **Finish** to save the configuration.
6. Add additional servers as required.

Viewing DRA Events in Change Guardian

You can view DRA Events in the Change Guardian Events Dashboard.

Viewing Change Guardian Reports in DRA

To view the Unified Change History reports on AD objects from Change Guardian, see “Utilizing Unified Change History” in the *Directory and Resource Administrator User Guide*.

Issues Coexisting with Change Guardian

Change Guardian events do not display the actual DRA user name in the following scenarios:

- When you define the computer account enabled or disabled, user account unlock policies.
- When you make any modifications in the Group scope or Group Type.
- When you make changes to the remote access permission in Dial In tab in DRA, two modification events are populated.The event shows User-Parameters in the delta.
- When you make changes in Azure AD and Exchange using DRA.
- When you make changes in the following tabs in DRA:
  - Account tab
  - Password tab
  - Member of tab
  - Terminal Services tab
  - Dial in tab
  - Call back tab

12 Advanced Management of Events

This advanced event management console allows you to search system events of severity 0 and 1 and view all events with severity 0 to 5. You can create a filter to search and save the search. You can generate various types of Change Guardian reports from templates or customize reports.

The advanced event management console provides the following functionalities:

- "Searching Events" on page 155
- "Managing Reports" on page 176
- "Filtering Events" on page 181
- "Tagging Events" on page 188
- "Executing Actions" on page 191
- "Viewing Vulnerabilities" on page 192
- "Emailing Event Details" on page 192
- "Searching in a Federated Environment" on page 192
- "Viewing Identity Data" on page 194

To view the advanced management console, open the following URL and click **ADMINISTRATION**:

```
https://<IP_Address_Change_Guardian_server:<port_number>
```

The default port is 8443. You can use a custom port if Change Guardian was installed with custom configurations.

For troubleshooting tips about using the advanced console, see "After Logging in to the Web Console, Opening ADMINISTRATION tab Displays Blank Page on Internet Explorer" on page 227.

Searching Events

Change Guardian provides an option to perform advanced search on events. With the necessary configuration, you can also search system events generated by Change Guardian and view the raw data for each event. By default, events are returned in a reverse chronological order.

Search results include all events generated by the Change Guardian system operations, by default. These events are tagged with the `Sentinel` tag. If you do not specify a query and click **Search** for the first time, the default search returns all events with severity 0 to 5. Otherwise, the search feature reuses the last specified search query.

You can run a search to view events indexed in traditional storage. You can also search for events in other Change Guardian servers that are distributed across different geographic locations.

To search for a value in a specific field, use the ID of the event name and the value. For example, to search for an authentication attempt to Change Guardian by user2, specify the following:
`evt:LoginUser AND sun:user2`

You can use advanced feature to refine searches using the product name, severity, source IP, and the event type. You can combine multiple advanced search criteria by using operators. The advanced search criteria syntax is modeled on the search criteria for the Apache Lucene open source package.

- To search events with the product name NMAS and severity five:

  `pn:NMAS AND sev:5`

- To search the initiator IP address 10.0.0.1 and a “Set Password” event:`sip:10.0.0.01 AND evt:"Set Password"`

NOTE: If time is not synchronized across your server, client, and event sources, you might get unexpected results from your search. This is especially a problem if searches are performed on time durations such as **Custom**, **Last 1 hour**, and **Last 24 hours** where display results are based on the time zone of the machine on which the search is performed.

Following sections provide information about the following:

- “Performing a Search” on page 156
- “Viewing Search Results” on page 157
- “Refining Search Results” on page 159
- “Saving a Search Query” on page 161
- “Exporting the Search Results to a File” on page 165
- “Search Query Syntax” on page 166

Performing a Search

To search:

1. In the **Reports and Searches** panel, click **New search**.
2. You can perform a search by using any of the following:
   - **Search criteria:** Specify the search criteria in the **Search** field.
   - **Build criteria:** Build a new criteria using the build criteria user interface.
   - **Select and Append criteria:** Click **Select and Append criteria** and select from the criteria listed, click **Add > Search**. You can select criteria from the list of criteria or filter the criteria based on recent criteria, tags, or filters.
     - **Show only recent criteria:** Select a search criterion from the recent search history. The search history displays a maximum of 15 search expressions. Select the criteria, click **Show recent criteria**, and then click **Add**.
     - **Show only Filters:** You can reuse existing filters to perform a new search. Click **Show Filters** that lists the existing filters. Select the filter on which you want to perform the search, and then click **Add**.
     - **Show only Tags:** You can search events that have a particular tag. Click **Show Tags**, that lists the tags in the system. Select the tags, and then click **Add**.

   You can combine multiple criteria, tags, or filters by using the **And** or **Or** condition.
3. (Optional) Select a time period for the search.
   - The default is **Last 1 hour**.

- **Custom** allows you to select a start date and time and an end date and time for the query. The start date should be earlier than the end date, and the time is based on the machine's local time.
- **Whenever** searches all available data, without any time constraints.

4 (Optional) If you have administrator privileges, you can select other Change Guardian servers for the search.

   If you have data federation configured, you can perform a search on other Change Guardian servers. For more information, see Chapter 10, "Configuring Data Federation," on page 143.

5 Click **Search**.

   The search results are displayed. For information on the search results, see "Viewing Search Results" on page 157.

6 (Optional) Modify the search criteria by clicking **Edit Criteria**.

7 (Optional) Modify the search results by selecting the desired event fields in the search results

   To add an AND or Or condition to the existing criteria, left-click the event field, select the required fields, and then specify the desired condition.

8 Click **Search**.

9 (Conditional) To save the search query, see "Saving a Search Query" on page 161.

Viewing Search Results

Searches return a set of events. When results are sorted by relevance, only the top 50,000 events can be viewed. When results are sorted by time, all the events in the system are displayed.

Occasionally, the search engine might index events faster than they are inserted into the data directory. If you run a search that returns events that were not added in the data directory, you get a message indicating that some events match the search query, but they are not found in the `data` directory. If you run the search again later, the events are added to the `data` directory and the search is shown as successful.

To see detailed event information, click the shield icon.

The information in each event is grouped into the following categories:

Category	Icon	Description
General	No icon	Generic information about the event, such as severity, date, time, product name, and taxonomy.
Initiator	↗	The source that caused the event to occur. The source can be a device, network port, etc.
Target	◎	The object that is affected by the event. The object can be a file, database table, directory object, etc.
Observer	👁	The service that observed the event activity.
Reporter	📝	The service that reported the event activity.
Tags	No icon	Tags that the events are being tagged with.
Customer value	No icon	Fields set by the customer.
Retention period	No icon	Retention period of the event.

The initiator, target, and observer can be hosts, services, and accounts. In some cases, the initiator, target, and observer can be all the same, such as a user modifying this or her own account. In other cases, the initiator, target, and observer can be different, such as an intrusion detection system detecting a network attack. If an event field has no data, it is not displayed in the results.

Event fields are grouped according to the following categories:

Group	Icon	Description
Host	🖥	The initiator or target host information. For example, initiator host IP, target hostname, or target host ID.
User	👤	The initiator or target user information. For example, the initiator username, initiator user department, target user ID, or target username.
Service	⚙	The initiator or target service information. For example, the target service name, target service component, or initiator service name.
Domain	🌐	Domain information of both the host and user. For example, the target host domain and initiator username.
IPCountry	⚑	The country information of the initiator and target trust. For example, the target host country.
Target trust	📇	The target trust and target domain information of the event that was affected. The name can be a group, role, profile, etc.
Target data	📄	The target data name and data container information. The data name is the name of the data object, such as a database table, directory object, or file that was affected by the event. The data container is the full path for data object.
Tenant name	🏠	The name of the tenant that owns the event data, applied to all the events in the inbound stream from a given Collector. The tenant name can be the name of the customer, division, department, etc.

Group	Icon	Description
Vulnerability	☣	A flag that indicates whether Exploit Detection has matched this attack against known vulnerabilities in the target.

Each event type is represented by a specific icon. The following table lists the icons that represent the various types of events:

You can view the search results in the summary view and in the detailed view. When you mouse over an event field, the information about the field is displayed.

Icon	Type of Event
⚙	Audit event
⏲	Performance event
⊞	Anomaly event
⏰	Correlation event
101 010	Unparsed event

Summary View

The Summary view of the search results displays the basic information about the event. The basic information includes severity, date, time, product name, taxonomy, and observer category for the event.

Detailed View

1. To view the report details, click the **More** link at the top right corner of the search results.

   This displays details such as host/user domain information, IPCountry information, extended target fields like TargetTrust and TargetData, Observer and Reporter fields, customer set variables, default data retention duration information for any individual event, and the tags set for the event.

2. To view all the details of an event, click the **All** link.

3. To view details about all events, click the **Show more details** link at the top of the search results page.

   You can expand or collapse the details for all events on a page by using the **Show more details** or **Show less details** link.

Refining Search Results

The search refinement panel can be used to narrow the search results by selecting one or more values for an event field. You can refine the results for one or more event fields.

The set of event fields that is displayed in the search refinement panel is configurable on a per-user basis.

For performance considerations, the maximum sample size used to calculate the event field value statistics is 50,000 events. The actual sample size is displayed in the field count label as `Field counts based on the first <sample-size> events` where `<sample-size>` is replaced by the actual sampling size.

To refine search results:

1. In the **Reports and Searches** panel, click **New Search**.
2. Specify the search criteria, then click **Search**.
3. Click **fields** in the REFINE section.The Select Event Fields window is displayed.
4. To refine the search, select the event fields from the available fields, then click **Save**.

   The selected event fields are displayed in the **REFINE** panel.

   A count at the right side of each event field displays the number of unique values that exist for that event field in the data directory. The calculation is based on the first 50,000 events found.

   The event field selection is on a per-user basis. Each user can have a different set of selected event fields.
5. Click each event field to view the unique values for that event field.

   For example, if the search results contain events that had severities 1, 2, 5, and 4, the event field is displayed as **Severity (4)**.

   The top 10 unique values are initially displayed in the order of most frequent to least frequent.

   The value next to the check box represents the unique value for that event field and the value at the far right represents the number of times the value appears in the search result.

   If there are multiple unique values occurring the same number of times in a search, the values are sorted by the most recent occurrence of the value.

   For example, if events of severity 1 and 4 occurred 34 times in the search results, and an event of severity 4 was logged most recently, the unique value 4 appears at the top of the list.

   To display the unique values in the order of least frequent to most frequent, click **reverse.**

   When there are more than 10 unique values, you can view and filter either the top 10 or the bottom 10 unique values. You cannot refine your search on both the conditions at the same time.

   In the following scenarios, the number of events returned from a refined search is greater than the number of values listed for an event field:

   - If the refinement performs a new search with additional terms intersected with the initial search string, such as by using an AND operator, the new search is run against all events in the system, including the result set from the initial search. If new events that came into the system match the refined search, they are shown in the resulting set and the event count is greater than the field value count.
   - If there are more than 50,000 events, the event field statistics are calculated only on the first 50,000 events.

     There could be an event field value that occurs 50 times in the first 50,000 events, but it could occur 1,000 times in all other stored events. In this scenario, the displayed value count is 50, but when the search is refined with this value it returns 1,000 events.
6. Click **OK**.

   Selected event field values are listed under the event field in the **REFINE** panel.

The right panel displays the refined search results, which contain only the selected values.

7. Repeat Step 3 through Step 6 to further refine the search.
8. (Optional) Click **clear** to clear the selected unique event field values from the **REFINE** panel and to return to the original search results.
9. (Optional) Click **add to search** to add the refined search values to the current search tab and to recalculate the search statistics.

   If you have already added the event field value to the current search tab, clicking **clear** does not return to the previous search results.

Saving a Search Query

You can save a search query, then repeat it as desired. To save a search query, you must first perform a search. When you are satisfied with the search results, you save the search query.

NOTE: You must have the necessary permission to access the specific options. For example, only users in the Report Administrator role can save the search query as a report template.

- "Saving a Search Query as a Search Template" on page 161
- "Saving a Search Query as a Filter" on page 161
- "Saving a Search Query as a Report Template" on page 162
- "Saving a Search Query as a Routing Rule" on page 164
- "Saving a Search Query as a Retention Policy" on page 165

Saving a Search Query as a Search Template

1. Perform and refine a search until you are satisfied with the search results.

   For more information, see "Refining Search Results" on page 159.
2. Click **Save as**, and then click **Save search**.
3. Specify a unique name for the search and provide an optional description.
4. Specify the following information in the **Default Parameters** section:

   Data sources: Displays the number of servers that Change Guardian will search for events. This option is useful if data federation is enabled. To select the data sources you want to search, click **selected data sources**, then select the data sources.

   Email to: To e-mail the report template to others, specify the e-mail address. To send the report template to more than one person, specify multiple e-mail addresses separated by a comma.

   Result limit: Specify the number of results to be stored in the search template. By default, 1000 results are stored in a report template.
5. Click **Save**.

Saving a Search Query as a Filter

You can save your search queries as filters for future use so you can perform a search using the saved filters rather than specifying the query manually every time.

To save a search query as a filter:

1. Perform a search, and refine the search results as desired.

   For more information, see "Refining Search Results" on page 159.

2. (Conditional) If you are using Change Guardian with traditional storage, click **Save as**, then click **Save search as filter**.

3. Specify a unique name for the filter and an optional description.

4. In the drop-down list, select one of the following options to specify the access for this filter:

   - **Private:** Allows you to make this filter private. Other users cannot view or access this filter.
   - **Public:** Allows you to share this filter with all users.
   - **Users in same role:** Allows you to share this filter with users who have the same role as yours.
   - **Users in selected roles:** Allows you to share this filter with users in specific roles. If you select this option, a blank field is displayed where you can specify the roles. As you type the role name, a list of roles is displayed.

     Select one or more roles.

     NOTE: This option is available only for users in the administrator role.

5. Click **Save**.

   The saved filter is listed in the Filters panel.

Saving a Search Query as a Report Template

You can save the search query as a search report.

NOTE: You must have the Manage Reports permission to save the search query as a report template.

1. Perform a search, and refine the search results as desired.

   For more information, see "Refining Search Results" on page 159.

2. When you are satisfied with the search results, click **Save as**, then click **Save search as report**.

3. Specify the following parameters:

Parameter	Description
Report name	Specify a unique name for the report. The name should not exceed 200 characters.
Based on	Select the base report from which you want to create the report. You can view a sample report by clicking the **View Sample** button.
Description	The description is automatically displayed based on the report that is selected and you can edit the description.
Criteria	Criteria is automatically populated based on the report selected and is not editable.

Parameter	Description
Additional criteria	Specify additional search criteria to the existing criteria. To build a new criteria on your own, click **Edit Criteria**. To build a new criteria from available system objects containing criteria, click **Add Criteria**. The criteria that you add here is appended to the existing criteria.
Data sources	Select the source machines on which the reports can be run by clicking the **selected data sources** link. You can select data sources only if your Change Guardian is configured for data federation. For more information, see Chapter 10, “Configuring Data Federation,” on page 143.
Additional Criteria	Specify additional criteria to refine the results. The criteria that you specify here can be edited while scheduling the report. If you specify **Criteria name**, the name is displayed at the end of the report results. **NOTE:** This parameter is not available for all reports.
Time Zone	Specify the time zone with which you want to populate the report. When you schedule the report, the time zone that you specify here is displayed in the report data. For example, if the Time Zone is set to US/Pacific-New time, the report data displays the selected time zone. By default, it displays the time zone that is set in the client system. **NOTE:** This parameter is not available for all reports.
Date Range	If the report includes time period parameters, choose the date range. All time periods are based on the local time for the browser. The **From Date** and the `To Date` automatically change to reflect the option you selected. ◆ **Current Day:** Shows events from midnight of the current day until 11:59:00 PM of the current day. If the current time is 8:00:00 AM, the report shows 8 hours of data. ◆ **Previous Day:** Shows events from midnight yesterday until 11:59:00 PM yesterday. ◆ **Week To Date:** Shows events from midnight Sunday of the current week until the end of the selected day. ◆ **Previous Week:** Shows events for the last seven days. ◆ **Month to Date:** Shows events from midnight the first day of the current month until the end of the selected day. ◆ **Previous Month:** Shows events for a month, from midnight of the first day of the previous month until 11:59:00 PM. of the last day of the previous month. ◆ **Custom Date Range:** Shows events for a period whose start and end date are chosen. If you select **Custom Date Range**, set the start date (**From Date**) and the end date (**To Date**) for the report.
From Date	Lets you set the from date.
To Date	Lets you set the to date.

Parameter	Description
Event Name	Name of the event. Default value is *
Severity	0 1 All
Email to	Specify an e-mail address in the **Email to** field. If you want to mail the report to more than one user, separate the e-mail addresses with a comma.
Result limit	Specify the number of results to be displayed or stored when you run or schedule the report. By default, 1000 results are stored. If you specify a value in **Group By** field, the result limit is based on grouping.

4. Click **Save** to save the search as report definition.

   You can see the saved report definition in the **Reports and Searches** panel.

Saving a Search Query as a Routing Rule

You must be in the administrator role to save the search query as a routing rule.

1. Perform a search, and refine the search results as desired.

   For more information, "Refining Search Results" on page 159.

2. When you are satisfied with the search results, click **Save as**, then click **Save search as routing rule**.
3. Specify a name for the rule.
4. (Conditional) To associate one or more tags to the events, click **Select tag**, select the desired tags, then click **Set**.
5. Select where you want to route the events to:
   - **All:** Events are routed to all Change Guardian services, including Correlation and Security Intelligence.
   - **Event store only:** Events are sent directly to the event store, and are not displayed in Event Views and the search results page.
   - **None (drop):** Events are dropped or ignored, and are not sent to any Change Guardian service.
6. Select one or more actions to be performed on each event that meets the search criteria. Click the plus and minus icons to add and remove actions.
7. Click **Save**.

Saving a Search Query as a Retention Policy

You must be in the administrator role to save the search query as a retention policy.

1. Perform a search, and refine the search results as desired.

   For more information, see "Searching Events" on page 155 and "Refining Search Results" on page 159.

2. When you are satisfied with the search results, click **Save as**, then click **Save search as retention policy**.

3. Specify a name for the retention policy.

4. In the **Keep at least** field, specify the minimum number of days to retain the events in the system. The value must be a valid positive integer.

5. (Optional) In the **Keep at most** field, specify the maximum number of days for which the events should be retained in the system.

   The value must be a valid positive integer and must be greater than or equal to the **Keep at least** value. If no value is specified, the system retains the events in the system until the space is available in primary storage.

6. Click **Save**.

   The newly created policy is displayed in the data retention table. For more information on retention policies, see Chapter 10, "Configuring Data Federation," on page 149.

Exporting the Search Results to a File

1. Perform a search, and refine the search results as desired.

   For more information,

2. In the search results, select the events you want to export to a file.

3. Click **Event operations** > **Export to file.**

4. Specify the following information:

   File Name: Specify a name for the file to which you want to export the search results.

   Event Limit: Specify the maximum number of events to be saved. The event limit must be less than the number of events you selected and the maximum event limit is 200000.

   All the search results are written into a `.csv` file. These files are then compressed into a `.zip` file for downloading.

5. (Optional) You can remove the event fields that you do not want to export to the file. Click **Choose Fields**, then clear the selections for the fields that you do not want to export to the file.

   By default, the null fields are excluded and not exported to file.

6. Click **Export** to export the search result to a file.

   A download file dialog box is displayed with an option to open or save the `.zip` file.

7. Select the desired option, then click **OK**.

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 about the event fields in Change Guardian, click **Tips** on the top right corner. A table is displayed that lists the event names and their IDs.

Use the following search query:

- "Basic Search Query" on page 166
- "Wildcards in Search Queries" on page 171
- "The notnull Query" on page 173
- "Tags in Search Queries" on page 173
- "Regular Expression Queries" on page 174
- "Range Queries" on page 174
- "IP Addresses Query" on page 175

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" on page 167
- "Special Characters" on page 167
- "Operators" on page 167
- "The Default Search Field" on page 168
- "Tokenized Fields" on page 169
- "Non-Tokenized Fields" on page 171

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 about quoting wildcard characters, see “Quoted Wildcards” on page 172.

Operators

Lucene supports AND, OR, and NOT Boolean operators, which allow words to be combined. Boolean operators must be always capitalized.

- “OR Operator” on page 167
- “AND Operator” on page 168
- “NOT Operator” on page 168
- “Operator Precedence” on page 168

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 user name or target user name 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 user name is admin and the target user name 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,obsdom,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 (initiator user name) and dun (target user name). 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 about tokenized fields in Change Guardian, click **Tips**. 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 172
- "Quoted Wildcards" on page 172
- "Leading Wildcards" on page 173

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 user name value contains the letters a, d, and m in sequence."
- **sun:*tester** The semantic is "find any event whose initiator user name value ends with "tester."
- **sun:*** The semantic is "find any event whose initiator user name 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 173.

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 167.

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 175
- "Wildcards in IP Addresses" on page 175

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"
```

Managing Reports

Reports help you analyze events to assess your compliance regulatory requirements, security best practices, and corporate IT policies. You can use reports to demonstrate compliance and manage information security risk.

Reports emphasize the event data and help you analyze events such as user account visibility, detection of possible security violations, account compromises, network security problems, and any other undesired activities. By analyzing reports, you can configure appropriate correlation rules and actions to prevent any possible non-compliance activities and vulnerabilities.

Consider a scenario where you have an IT policy that states to remove access rights of all employees to information and information processing facilities upon termination of their employment. To view all deleted, and disabled user accounts, and revoked accesses, you can run a report that displays the desired information in a few clicks. You can also schedule the report to run periodically at specific intervals.

You can generate various types of Change Guardian reports for administration and auditing purposes. When you run a report, you can accept or customize the default options, including:

- The frequency you want to run the report
- The name for the report
- A date range for events
- A specific event type

- A specific policy
- View all events, only managed events, or only unmanaged events
- View all change events, only successful change attempts, or only failed change attempts
- View events of a specified severity range
- Send the report to a specified email address

  For information about setting up email notifications, see "Configuring Email Servers" on page 72.

This chapter provides information about the following:

- "Creating Reports" on page 177
- "Scheduling Reports" on page 178
- "Working with Reports" on page 179
- "Rebranding Reports" on page 180
- "Running Reports in a Federated Setup" on page 181

Creating Reports

A report is a template that is combined at run-time with a number of criteria, such as time parameters, user security filters, other filter criteria for the events to be displayed in the report. A single report may have numerous associated report results. Reports can range from a simple list of events to multiple graphs and tables.

You can manage the reports and report results in the **Reports and Searches** panel. To manage reports, you must have the **Manage Reports** permission.

You can also create new reports in the following ways:

- **Using an Existing Report:** You can create a new report based on existing reports. These reports include predefined criteria for the events to be displayed in the report. To create a new report, select the report based on which you want to create a new report, click **Create report**, and then add additional criteria to suit your requirements.

  NOTE: You can create new reports only from reports created by users in the same role as yours.

- **Using a Search Query:** You can save your search query as a new report.

  NOTE: While saving a search query, ensure that you select the relevant option under **Based On**. Each option under **Based On** creates filters in the search query.

Scheduling Reports

To view the report result, you must run the report. All reports have a sample report result. You can use the sample report to preview how the actual report result looks like when you run the report. To run the report, you must have the **Run reports** permission.

You can run the report immediately or schedule it to run periodically. Click the **Run** icon and specify the appropriate information to schedule a report. By default, Change Guardian saves the report in the PDF format.

Reports run asynchronously.Therefore, you can simultaneously perform other tasks while the report generation is in progress. If the Change Guardian server is restarted while the report generation is still in progress, you can either cancel or reschedule report generation. If you reschedule the report, it runs with the same parameters that you used initially. If you schedule a report with a relative time setting, such as Week to Date, the time period for re-running the report is based on the current date and time and not the date and time when you initially scheduled the report.

NOTE: The report data in the PDF file will be different than the data in the reports that are run with the **Now** option. The report data in the PDF file are for the time range that you specified while scheduling a report definition. When you schedule a report definition with the **Now** option, the report includes events from midnight to the time you scheduled the report definition.

Scheduling Reports Across Change Guardian Servers

You can schedule reports on Change Guardian servers distributed across different geographic locations. For more information, see "Running Reports in a Federated Setup" on page 181.

Saving Reports in the CSV Format

You can also save a report in the CSV format along with the existing PDF format. This requires additional configuration in the Change Guardian server. Only users in the administrator role can perform the additional configuration. For more information, see "Generating a Report in CSV Format" on page 178.

Generating a Report in CSV Format

By default, Change Guardian generate reports in PDF format. You can also generate reports in CSV format by making additional configurations to the Change Guardian server.

To generate a report in CSV format:

1. Log in to the Change Guardian server as `root` user.
2. Change to novell user:

   ```
   su novell
   ```
3. Change directory:

   ```
   cd /etc/opt/novell/sentinel/config/
   ```
4. Open the file for editing:

   ```
   vi obj-component.JasperReportingComponent.properties
   ```

5. Edit the following entries:
   - `reporting.csv.enable=true`
   - `reporting.csv.outputdir=`*<the directory where the reports must be stored>*

   The `novell` user must have read and write permissions on the specified directory.
6. Change to `root`:

   `su root`
7. Restart the Change Guardian server.

When you generate a report, it is stored in the CSV format in the directory specified in the `reporting.csv.outputdir` attribute.

Working with Reports

The data that you view in reports depends on the security filter applied to your role. For example, if the security filter for your role is set to view events of severity 1 to 3, your report results will include only those events, although the report parameters allow severity 4 and 5 events also.

As you work with reports, you can perform several tasks including the following:

- **Finding Reports:** Change Guardian provides a large number of reports. You can use one of the following ways to easily find the reports you are interested in:
  - Using a particular keyword in the report name or description.
  - Using Tags.
  - Viewing reports belonging to a specific category: Scheduled or Unread.
- **Grouping:** To simplify report management as the number of reports grows over time, by default, Change Guardian groups the reports by **Category**.

  You can change the grouping to **None** if you want to list all your reports and searches under one heading. To change the grouping, click **More options**, select **Group by**, and then select the necessary option.
- **Tagging:** You can associate reports with existing tags. When a tag is set on a report, the report results associated with the report inherit the tag by default.
- **Marking reports and searches as Favorites:** You can mark the most frequently used reports and searches as Favorites to make them easier to find. You can also store them in folders to locate and manage them easily.
- **Drilling down into the reports to further analyze the data:** You can view events directly for a report without scheduling the report. The search results provide a preview of what to expect when you generate a report and the ability to investigate further. To view events for a report, click **Search Events**.
- **Sharing reports with other roles:** The **Share** functionality allows you to share reports with other roles and also control who can access your reports.

  For example, the out-of-the-box report templates are accessible to all Change Guardian users. Consider a scenario where you have several groups in your organization such as system administrators, database administrators. Because of the sensitivity of the audit data available in the report results when you run the out-of-the-box report templates, you may want to ensure that these administrators do not gain access to any unauthorized data. In such a scenario, you can restrict the report templates visibility only to you, to users in your role, or to users in selected roles.

NOTE: Only users in the Administrator role can restrict the visibility of the out-of-the-box reports.

For example, consider a scenario where there is a dedicated audit team in your organization whose primary job is to analyze and validate the accuracy of reports. You may want them to only view your reports but not modify or delete reports. In such a scenario, you can share your reports with the audit team. The audit team will only be able to view or run the reports depending on the permission they have. However, they will not be able to modify or delete reports.

To share reports, you must have the **Share reports** permission. To share reports with users in other roles, you must have the **Manage roles and users** permission in addition to the **Share reports** permission. You can share only the reports that you create. You cannot share reports that other users have shared with you. To share a report, select the report you want to share, click the **Share** icon, and select the relevant sharing option.

The events in the report results that users, with whom you have shared reports, can view depend on the permission their role has. For example, if their role has permission to view only events of severity 4 and 5, the report results include only those events.

If the user account of a report owner is deleted, reports that are set as **Private** are deleted. The ownership of all the shared reports is transferred to the admin user. If that report owner had shared any reports with you, you can no longer view those shared reports unless the admin user shares those reports with you.

Rebranding Reports

Change Guardian delivers an out-of-the-box Change Guardian white label report template. By customizing this template, you can rebrand the reports with your own header, footer, and logo. Only users in the administrator role can customize the Change Guardian white label report template.

To customize the template, perform the following:

1. In the **Reports and Searches** panel, select the Change Guardian White Label Template report definition, and then click Export.
2. Save the file to your local computer.
3. Create a new folder.
4. Extract the file contents to the new folder by using any ZIP extraction tool.
5. In the new folder, open the **resources** folder. In this folder, you can modify the following files:
    - **Header/Footer.jrxml**: Contains the report layout descriptions. You can modify the layout of fields, text, or images in the header and footer, but you must ensure that the overall size of the header and footer does not change. You can manually edit the XML file or use iReport to

      modify them.

- **Header/Footer*.properties**: Contains the text in the layout file, which localized into various languages. You can modify the strings that appear in the header or footer by editing this file. Ensure that the new strings do no exceed the space allocated to them. For information about editing the `.properties` file, see Oracle Java documentation.
- **Logo.jpg**: Contains the logo that appears in the footer. You can replace this file with another image. Ensure that the size of the new image is exactly the same size of the existing image.

6 Use a ZIP tool to re-zip the modified report template.

7 In the **Reports and Searches** panel, click Import reports or searches, browse to this zip file, and then click Import.

NOTE: If the folder structure is different than the original ZIP file, the import process displays an error. Ensure that you do not modify the folder structure after making the changes.

8 Schedule any report definition and view the report to ensure that the changes are applied correctly.

Running Reports in a Federated Setup

To run reports in a distributed environment, select the data source server from which you want to view reports and specify the report parameters. For more information, see "Searching in a Federated Environment" on page 192.

To run reports:

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**.

3 Click the **Data sources** link.

4 Select the data source servers from which you want to view reports, then click **OK**.

5 Specify parameters based on which to generate the report.

6 Click **Run**.

A report results entry is created and listed under the selected report.

Filtering Events

The Filters feature in Change Guardian allows you to customize the event search and prevent data overload. You can save a search query as a filter and reuse it as required, so that you can perform a search by selecting the filter rather than specifying the query manually every time.

Following sections provide information about configuring filters.

- "Creating Filters" on page 182
- "Sample Filters" on page 186
- "Viewing Events by Using Filters" on page 188
- "Managing Filters" on page 188

You can reuse filters while using or configuring Change Guardian features, such as:

- Configuring Data Synchronization
- Configuring a Data Retention policy.
- Configuring the data visibility settings for a role.
- Creating dashboards.
- Configuring event routing rules.
- Viewing real-time events in Event Views.

Change Guardian provides a list of filters by default. You can also create your own filters. To view the Filters available in Change Guardian, click **Filters** on the left navigation panel.

- **My Filters:** Lists the default filters and the filters you created.
- **Shared Filters:** Lists the filters that other users have shared with you.

Creating Filters

Filter criteria are simple math expressions and simple evaluations. Filters work on selection sets by matching events against the specified criteria. If the match is TRUE, the event is displayed in real-time views or search results, or passed to other functions. If the match is FALSE, the event is blocked. The filter criteria is your search query.

For example, consider a search query that is written as follows:

```
(sip:"10.0.0.1")
```

Events whose source IP address is 10.0.0.1 are included in the filter.

You must use the event field ID to represent an event name. Click the **Tips** for a list of event field names and their IDs.

Following sections provide information about creating filters.

- “Building a New Criteria” on page 182
- “Selecting an Existing Criteria” on page 184
- “Creating a Filter” on page 184

Building a New Criteria

The Build criteria interface provides a list of parameters required to build filter criteria ranging from simple to complex. You can either select the parameters, or you can manually specify the filter criteria.

The Build Criteria dialog box includes the following elements:

Table 12-1 Build Criteria Dialog Box Elements

Element	Description
Criteria	If you select **Structured**, this field displays the criteria formed by the parameters you select. You cannot modify or specify the filter criteria. If you select **Free-form**, you can manually specify the filter criteria.
Structured	Allows you to select the various parameters to build the filter criteria.
Free-form	Allows you to manually specify the filter criteria rather than selecting from the available parameters. The search criteria is based on the standard Lucene syntax with some Change Guardian extensions. If this option is selected, the following elements are not displayed: ◆ Event fields ◆ Criteria fields ◆ Field details
Exclude system events	Select this option to exclude Change Guardian internal events such as audit events and performance events from the search results.
Event fields	Displays a categorized list of possible event fields you can add to the filter criteria. You can expand each category to display the set of fields in that category. If you know the name of the field you want, specify the name in the **Search** field. The event category list will adjust to present only matching fields. For more information on event fields, click **Tips**..
Criteria fields	Lists a set of overlay criteria that you can use on top of per-field searches. The following fields are displayed by default: ◆ **All data:** Performs a search across all event fields. ◆ **Tags:** Events can be tagged in various ways to help identify relationships between events. Queries that include a “Tags” search will look at the event tags (rv145) for matches. ◆ **Taxonomy:** Events are also classified using a number of taxonomic categories for the action, outcome, and so on. Queries that include a “Taxonomy” search will search for specific classes of events.

Element	Description
Field details	The fields in this section vary depending on the event or criteria fields you select. For example: ◆ For tokenized fields, you can specify the words that you want to include or exclude in the filter criteria. For information on the tokenized and non-tokenized fields, click **Tips**. ◆ For non-tokenized fields, you can specify a value or a range of values. ◆ For taxonomy fields, specific taxonomy options are displayed. ◆ For date attributes, a date-time calendar is displayed as you type the date. You can select a date. ◆ For fields that contain internal Change Guardian UUIDs, such as the CollectorID field, the corresponding Change Guardian object names are displayed and can be selected.
Condition: AND OR	Allows you to specify the AND or OR condition between the criteria fields. These options are available when you add additional event criteria to the criteria fields.

Selecting an Existing Criteria

You can create a filter by using existing criteria from the predefined criteria list. The filter can be based on recent criteria, tags, or existing filters.

- **Show only recent criteria:** Select a search criterion from the recent search history. The search history displays a maximum of 15 search expressions. Select the criteria, click **Show only recent criteria**, and then click **Add**.
- **Show only tags:** You can search events that have a particular tag. Click **Show only tags** to list the tags in the system. Select the tags, and then click **Add**.
- **Show only filters:** You can reuse existing filters to perform a new search. Click **Show only filters** to list the existing filters. Select the filter on which you want to perform the search, and then click **Add**.

You can combine multiple criteria, tags, or filters by using the **And** or **Or** condition. After adding the criteria, you can test the filter by clicking **Test Filter**.

Creating a Filter

You can create filters either by building a new filter criteria or by saving a search query as a filter.

While creating a filter, you can specify whether you want to share a filter with other users. You must have the **Share Search Filters** permission to share filters with everyone or with users in the same role as yours. If you are a user in the administrator role, you can share filters with users in a different role.

Creating a Filter by Using the Build Criteria Dialog

1. In the navigation panel, click **Filters > Create a filter**.
2. Select one of the following methods to create a filter criteria:
    - To build the filter criteria by selecting parameters, make sure that **Structured** is selected, select the parameters, then continue with Step 3.

      For information on these parameters, see Table 12-1, "Build Criteria Dialog Box Elements," on page 183.
    - To manually specify the filter criteria rather than selecting the listed parameters, select **Free-form**. In the **Criteria** field, specify the filter criteria, then continue with Step 3.

      For information about the syntax for the criteria, see "Building a New Criteria" on page 182.
3. (Conditional) If you do not want to include Change Guardian internal events in the search, select **Exclude system events**.
4. Click **Search** to search events according to the specified filter criteria.

   By default, the search is performed on events that were generated within the last 1 hour.
5. Review the search results to verify that the filter is retrieving the expected events.
6. (Optional) You can modify the search query by selecting one or more event field values from the search results, or you can click **Edit search filter**, then make necessary changes.
7. When you are satisfied with the search results, click 💾▾, then click **Save as Filter**.
8. Specify a name for the filter and an optional description.
9. In the **Sharing** drop-down list, select one of the following options to specify the access for this filter:
    - **Private:** Allows you to make this filter private. Other users cannot view or access this filter.
    - **Public:** Allows you to share this filter with all users.
    - **Users in same role:** Allows you to share this filter with users who have the same role as yours.
    - **Users in selected roles:** Allows you to share this filter with users in specific roles. If you select this option, a blank field is displayed where you can specify the roles. As you type the role name, a list of roles is displayed.

      Select one or more roles.

   NOTE: This option is available only for users in the administrator role or users with the **Share search filters** permission.
10. Click **Save**.

Creating a Filter by Using a Search Query

You can save a search query as a filter and use this filter to perform searches when required rather than specifying the search query again. For more information about creating a filter by using a search query, see "Saving a Search Query as a Filter" on page 161.

Sample Filters

This section lists a few examples on how you can create filters.

- "View Events of Severity 3 to 5 from a System in China" on page 186
- "Determine if User "Bob Smith" Tried to Log In after His Account was Disabled" on page 186
- "View Events from Two Subnets and Share the Filter with Network Administrators" on page 187
- "Find all Events that Include the Words "database" and "service," and exclude "test"" on page 187

View Events of Severity 3 to 5 from a System in China

- Click **Build Criteria** > **Event fields**, select **SourceHostCountry**.
- The name should match any string that contains the name "China." For example, "ChinaBeijing." Specify `china*` in the **Value** field.
- The severity of the events must be 3 to 5:
  - In **Event fields**, select **Severity**.
  - In the **Values that range from** field, specify 3 TO 5.

NOTE: If you are familiar with the search query syntax, you can directly specify the query in the **Criteria** field as follows:

```
(rv29:china*) AND (sev:[3 TO 5])
```

Click **Search** to view events that match the specified criteria.

Determine if User "Bob Smith" Tried to Log In after His Account was Disabled

- Click **Build Criteria** > **Event fields**, select the following:
  - **InitiatorUserName**
  - **TargetUserName**
  - **EffectiveUserName**
- Select the **OR** condition.
- Specify `"Bob Smith"` in the **Value** field.
- To determine if the user has logged in, or tried to log in, select **Taxonomy** in **Criteria fields.**

  NOTE: You can also select the appropriate event fields if you are familiar with the values to be specified for the event fields. Taxonomy is a classification of events where events of similar type are grouped together. It helps you search events based on the taxonomy classification rather than you specifying the specific event names and their values.

- In the **Field details**, select the following:
  - From the **Class** drop-down list, select **User Session Events**.

  - From the **Identifier** drop-down list, select **Create**.
  - For **Outcome**, select **Success**, then select **Failure**.

NOTE: If you are familiar with the search query syntax, you can directly specify the query in the **Criteria** field as follows:

```
(xdasclass:2 AND xdasid:0 AND (xdasoutcome:0 OR xdasoutcome:1)) AND
(iufname:"Bob Smith")
```

Click **Search** to view the events that match the specified criteria.

View Events from Two Subnets and Share the Filter with Network Administrators

- Select subnets:
  - Click **Build Criteria** > **Event fields**, select **SourceIP**.
  - In **Field details** > **Value**, specify the subnet, for example, 172.17.0.0/16.
  - Repeat the above two steps to specify another subnet.
- The events must be from either of the subnets. Therefore, select **OR** as the condition.
- Click **Search** to view events that match the specified criteria.
- The filter must be shared with network administrators:
  - In the search results panel, click 💾▾, then click **Save as new filter**.
  - Specify an intuitive name and an optional description.
  - From the drop-down list, select **Share with roles**, then select **Network Administrator**.
- Click **Save**.

Find all Events that Include the Words “database” and “service,” and exclude “test”

- Click **Build Criteria** > **Criteria fields**, select **All data**.
- You want to find events that include words “database” and “service,” and exclude “test.” Therefore, in **Field details**, specify the following:
  - In the **All of these words** field, specify `database service`.
  - In the **Exclude these words** field, specify `test`.

NOTE: If you are familiar with the search query syntax, you can directly specify the query in the **Criteria** field as follows:

```
_data:(database AND service) NOT _data:test
```

The `_data` field allows you to search for words that might appear in any event field.

Click **Search** to view the events that match the specified criteria.

Viewing Events by Using Filters

You can use filters to view events either by selecting the desired filter in the **Filters** panel or by using the **Filter** icon in the search results panel. For more information, see "Searching Events" on page 155.

Managing Filters

You can edit and delete only the filters that you created. The default filters and the filters that other users have shared with you cannot be edited or deleted.

Tagging Events

Tags are user-defined values that can be used to logically group data collection objects such as event routing rules, report templates, and report results. Tags help you to filter object lists for the data collection objects and also to augment incoming data. You can search for events, report templates, and report definitions that are tagged with a particular tag.

You can associate objects with more than one tag. You can, for example, create tags related to regulations (PCI) or compromised systems or network infrastructure such as routers, switches, and firewalls. Some organizations need to define data retention or data viewing policies based on the geographic location, so tags can be used to tag event sources based on different locations.

The **Tag** icon allows you to quickly add tags to the desired data collection objects such as report templates, and report results.

Following sections provide information about tagging:

- "Creating a Tag" on page 188
- "Viewing Tagged Events" on page 189
- "Managing Tags" on page 189
- "Performing Text Searches for Tags" on page 190
- "Deleting Tags" on page 190
- "Associating Tags with Objects" on page 191

Creating a Tag

To create a tag:

1. Select **Tags** in the navigation panel on the left or click the **Tag** icon in the appropriate data object interface to which you want to associate tags.
2. Click **Create**.
3. Specify a name for the tag.

   Tags have the following naming conventions, and a warning message is displayed if the name you specify does not comply with the following conventions:

   - Tag names should not be more than 20 characters.

    - There should not be any white space as part of the tag name.
    - A tag name is not case-sensitive. You cannot create two tags with identical names except for capitalization. For example, you cannot have the tag names `IDM` and `idm`, because both are perceived as the same name.

4. Specify an optional description for the tag.

   If the tag name is available, a message is displayed.

   If a tag with the same name already exists, a message is displayed indicating the name is not unique. You must specify a different name for the tag.
5. Click **Save**.

Viewing Tagged Events

You must have the appropriate permission to view events that are tagged with specific tags. For example, only users in the PCI Compliance Auditor role can view events that are tagged with at least one of the regulation-related tags such as PCI, SOX, HIPAA, NERC_CIP, FISMA, GLBA, NISPOM, JSOX, and ISO/IEC_27002:2005.

To view tagged events, do any of the following:

- From the Tags panel, select the tag for which you want to view events, then select **Search**.
- In the **Search** field, click the **Tag** 🏷 icon, select the desired tags, then click **OK**. Click **Search**.
- In the **Search** field, specify `rv145:<tagname>` or @<tagname> as the search criteria, then click **Search**.

Managing Tags

You can add and remove to favorites, view, edit, and sort tags

Following section provide information about managing tags.

- “Adding and Removing Tags from Favorites” on page 189
- “Sorting Tags” on page 190
- “Viewing and Modifying Tags” on page 190

Adding and Removing Tags from Favorites

You can add your frequently used tags to the Favorites section so that it is easier to locate them and associate them with objects. When a tag is added to the Favorites section, it is removed from the Other section.

To add or remove a tag from Favorites:

1. Log in as a user in the Manage Tags role.
2. Select **Tags** in the navigation panel on the left.
3. To add or remove a tag from Favorites, select the tag, then click the **Favorites** ★ icon.

Sorting Tags

You can sort tags either based on their names or based on the number of objects associated with the tags.

To sort tags:

1. Log in as a user in the Manage Tags role.
2. Select **Tags** in the navigation panel, then click **More**.
3. (Conditional) To sort the tags in the alphabetical order, select **Sort by Name**.
4. (Conditional) To sort the tags based on the number of objects associated with them, select **Sort by Count**.

The Tags are sorted according to the selection.

Viewing and Modifying Tags

You can modify only the description of a tag.The tag name cannot be modified because it might be used to tag events and other data collection objects, and it is not an accepted practice to modify events that are already stored. Therefore, to modify the name of a tag, you must create a new tag.

To view or modify a tag:

1. Log in as a user in the Manage Tags role.
2. Select **Tags** in the navigation panel on the left.
3. Select the tag that you want to edit, and click the **Edit** ✎ icon.
4. Modify the description as necessary, then click **Save**.

Performing Text Searches for Tags

This option is useful when you want to look for a particular tag.

To search a tag:

1. Log in as a user in the Manage Tags role.
2. Select **Tags** in the navigation panel on the left.
3. To search for a particular tag, specify the name or description of the tag or a keyword. To search for multiple tags, specify the tag names separated by the space character.

   The tag that matches the keyword is displayed.

Deleting Tags

To delete a tag:

1. Log in as a user in the Manage Tags role.
2. Select **Tags** in the navigation panel on the left.
3. Select the tag that you want to delete, then click the **Delete** 🗑 icon.

The Change Guardian tag is a system tag that tags all Change Guardian internal events, and cannot be deleted.

4 Click **Delete** to confirm deletion.

Associating Tags with Objects

- "Associating Tags with Event Routing Rules" on page 191
- "Associating Tags with Report Results and Report Definitions" on page 191

You can associate tags with event routing rules, and reports and report templates. You can add more than one tag to a data collection object. However, the `rv145` field, which stores the tag value, can hold a maximum of 256 characters. Therefore, the maximum number of tags that you can associate with an object depends on the length of the tag name.

Associating Tags with Event Routing Rules

To associate tag with event routing rules:

1. Click **Routing** in the toolbar, then click **Create**.
2. Specify a name and filter criteria for the rule.
3. Click **Select tag**, then select the tags that you want to associate with the rule.
4. Click **Set**.

Associating Tags with Report Results and Report Definitions

NOTE: When a tag is set on a report definition, the report results under the report definition inherit the tag by default. Inherited tags for a report result appear disabled in the Tag selector dialog box.

To associate a tag with reports:

1. Select **Reports** in the navigation panel on the left.
2. Select the report result or the report definition that you want to associate with a tag.
3. Do one of the following:
    - Select **Tags** from the **more** drop-down list.
    - Click **Edit** at the bottom left pane.
4. Select one or more tags that you want to associate with selected reports.
5. Click **Set**.

Executing Actions

Users in the following roles can execute actions on events:

- Security Policy Administrator
- User

You need to configure the actions before executing actions on events.

To execute actions on events:

1. Perform a search, and refine the search results as desired.

   For more information, "Performing a Search" on page 156.
2. In the search results, select the events on which you want to execute actions.
3. Click **Event operations** > **Show action panel**.
4. In the **Event Actions** panel > **Actions** drop-down, select the desired actions, then click **Execute**.

   The results of the actions are displayed in the **Results** field.

Viewing Vulnerabilities

You must have the View asset vulnerability data permission to view the Vulnerability data. You can view the vulnerabilities of the selected destination systems. To view the Vulnerability data, you must run the Vulnerability Collector and ensure that the Vulnerability scan information is being added to the Change Guardian database.

Vulnerabilities can be seen for the current time or for the event time.

- **View Vulnerabilities at current time:** This report queries the database for vulnerabilities that are active (effective) at the current date and time, and displays the relevant information.
- **View Vulnerabilities at time of event:** This report queries the database for vulnerabilities that were active (effective) at the date and time of the selected event, and displays the relevant events.

To view the Vulnerability report:

1. Perform a search, and refine the search results as desired.
2. In the search results, select the events for which you want to view the Vulnerability data.
3. (Conditional) To view vulnerabilities at the current time, click **Event operations** > **View Vulnerabilities at current time**.
4. (Conditional) To view vulnerabilities at the time of the event, click **Event operations** > **View Vulnerabilities at time of event.**

Emailing Event Details

To email event details to other users, you must configure SMTP. For more information, see "Configuring Email Servers" on page 72.

Searching in a Federated Environment

- "Understanding Data Federation" on page 193
- "Searching for Events" on page 193
- "Managing Search Results" on page 193

Understanding 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. When data federation is enabled, you can perform a search or run a report on one server and have it automatically run a search or report across the selected remote servers.

For information about reports and alerts in a data federated environment, see "Running Reports in a Federated Setup" on page 181 and.

Searching for Events

In a distributed environment, you can search for events on the selected data source servers and also the local server.

To search for events:

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.
4. Select the data source server 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.

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. The search results are filtered through a 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.

NOTE: For the data source servers search results are based on the role of the authorized requestor server and not on the role of the logged-in user that is performing the search.

The Extended Status page displays the progress and status of a search query. To access the Extended Status page, click the **Displaying N of M events from X data sources** link from the refinement panel.

The extended status page displays the following information:

- **Data Source Name:** The name of the data source server, if specified. If you did not specify a name, it displays the IP address or the DNS name of the data source server.
- **Events Available:** The number of events that were retrieved from the data source server out of the total number of events that matched the search criteria.
- **Retrieval Rate (EPS):** An approximate rate with which the events were retrieved from a specific data source server.

- **Status:** Any of the following status of the search queries and error messages, if any:
  - **Running:** Indicates that the search is still running on the data source server.
  - **Buffering events for display:** Indicates that the search is completed, 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 completed, but the authorized requestor has paused retrieving events from the data source. When the authorized requestor 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 the result is retrieved by the authorized requestor and queued for display.

Each event displays information about the data source server from which the event is retrieved. To view details about events, click the **All** link to expand event results.

If the role of your security filter is set to view all event data, the **get raw data** link is displayed. Click this link to view non-internal events.

Viewing Identity Data

This section provides information about integrating Change Guardian with Microsoft Active Directory (AD). This integration helps you identify the usernames associated with an event. You must synchronize the AD accounts with the AD server. For more information, see "Configuring LDAP for Authentication" on page 63.

You can view identity data by clicking **People** on the left pane.

This section provides the following information:

- "Performing a Search" on page 194
- "Viewing Profile Details" on page 196
- "Viewing Activities" on page 196
- "Searching and Viewing User Identities" on page 196

Performing a Search

The People Browser allows you to search for people to view what they have been doing. You can use the search box or click the arrow next to the search box for more options. As you start typing the information in the search field, the data is automatically displayed.

You can search for users by using the search box or by using the search fields.

- "Using the Search Box" on page 195
- "Using the Search Fields" on page 195

Using the Search Box

The search box automatically uses the following logic to interpret the text you enter:

- All letters and no spaces searches for the given name or surname.
- All letters and a space between letter groups searches for the given name and surname. The surname match is a starts-with, unless there is a trailing space.
- All letters with a comma in the middle is a match of the surname and given name. The given name match is starts-with unless there is a trailing space.
- Anything with a @ in it is a starts-with match for e-mail address.
- All digits, or letters and digits but no telephone punctuation characters is a starts-with match for workforce ID.
- Digits in addition to a leading +, and spaces, hyphens, periods, or parentheses is a starts-with match for a telephone number.
- Alphanumeric, or all numeric with no spaces, or all numbers with spaces is a starts-with match for the workforce ID.

Using the Search Fields

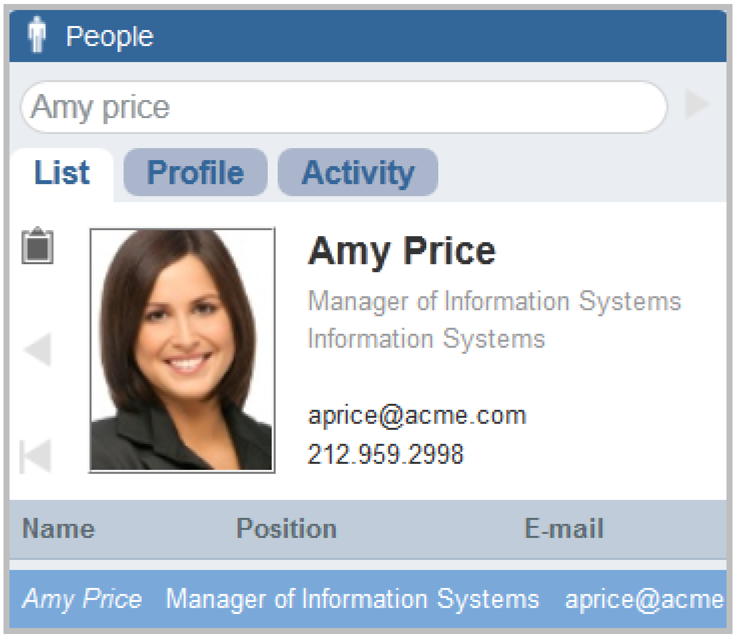
You can search for many values, including custom values, in the search fields. The following is a list of the fields you can search:

- Given Name
- Surname
- Telephone
- Email
- Position
- Department
- Office Location Code
- Workforce ID
- Vault Name
- Customer ID
- DN
- Custom Value Name
- Custom Value

Viewing Profile Details

After you have performed the search, (see "Performing a Search" on page 194), the user name, photo, position, department, e-mail, and telephone number are displayed.

Figure 12-1 User Information Displayed



Amy Price
Manager of Information Systems
Information Systems

aprice@acme.com
212.959.2998

Name	Position	E-mail
Amy Price	Manager of Information Systems	aprice@acme

You can also view detailed information about the user and all of the accounts that belong to this user.

You can use the clipboard functionality to copy the data of the user's profile and account information. Click the clipboard icon to the left of the user's photo and their information is now in the clipboard. You can paste this information into a text editor.

Viewing Activities

You can view the recent activity of a user through the People Browser.

- Authentication information
- Access events
- Permission changes

Searching and Viewing User Identities

The People Browser in Change Guardian allows you to search and view user profiles of identities in the Change Guardian database that have been synchronized with AD. In addition to information from the identity management system, the People Browser also shows recent user activity collected by Change Guardian.

13 Backing Up and Restoring Data

The Change Guardian backup and restore utility is a script that performs a backup of Change Guardian data and also allows you restore the data at any time on the Change Guardian server.

NOTE: You can restore data only on the same version of Change Guardian in which the data was backed up. Restoring data between different Change Guardian server versions might cause data incompatibility due to changes between the product versions. Similarly, you can restore data only on the same type of data storage using which the data was backed up. For example, data that you back up in traditional storage can be restored only in traditional storage.

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 that 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. 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.

This chapter provides the following information:

- "Parameters for the Backup and Restore Utility Script" on page 198
- "Running the Backup and Restore Utility Script" on page 200
- "Restoring Data" on page 202

Parameters for the Backup and Restore Utility Script

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

Table 13-1 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 `./cgbackup_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 `./cgbackup_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 that are created and assigned, alert configurations, event dashboard configurations. **NOTE:** When you perform a full system backup or configuration data backup using this parameter, restore the data on the same version of Change Guardian with the same type of data storage using which the data was backed up. Restoring data between different Change Guardian server versions might cause data incompatibility due to changes between the product versions.
`-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.

Parameters	Description
-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.
-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 because 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.
-A	Backs up alerts and the events that triggered the alert.
-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 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.

Prerequisites:

- Ensure that the time and timezone is same on both the source machine from where the backup is taken and the destination machine where the restoration of data will happen.
- Ensure that the IP address of both the source and destination machines are the same.

To backup and restore:

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

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

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

   For more information about different parameters, see Table 13-1. 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.

Syntax	Action
./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.
./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 `cgbackup_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 202.

NOTE: When you perform a full system backup or configuration data backup using the parameter `-c`, restore the data on the same version of Change Guardian with the same type of data storage using which the data was backed up. Restoring data between different Change Guardian server versions might cause data incompatibility due to changes between the product versions.

Restoring Data

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

- "Enabling Event Data for Restoration" on page 202
- "Viewing Event Data Available for Restoration" on page 202
- "Restoring Event Data" on page 203
- "Configuring Retention Period" on page 204

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/sentinel/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, click **ADMINISTRATION** in the web console and search. In the Search results, click **All** for any local event.

Viewing Event Data Available for Restoration

1. Log in to the Change Guardian web console as a user in the administrator role, and click **ADMINISTRATION**.
2. Click **Storage > Events**.

   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 Data" on page 202 to restore the event data.

Restoring Event Data

1. Select the check box in the **Restore** column next to the partition 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 202.

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.

14 Upgrading Change Guardian Server

This chapter provides information about the following sections:

Upgrade Checklist

Use the following checklist to upgrade your Change Guardian installation:

Table 14-1 *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.	Supported platforms on the System Requirements page.
❐	Understand the order for the upgrade before upgrading the operating system on the Change Guardian server,	"Upgrading the Appliance Installation" on page 208
❐	Review the SUSE Release Notes for known issues related to the supported operating system.	SUSE Release Notes
❐	Review the Change Guardian Release Notes to see the new functionalities and understand the known issues.	Release Notes
❐	Upgrade the Change Guardian server.	◆ "Upgrading a Traditional Installation" on page 206 ◆ "Upgrading the Appliance Installation" on page 208 **IMPORTANT:** You must upgrade the Change Guardian server and Policy Editor. However, the Change Guardian Agent for Windows is backward compatible.

	Tasks	See
❒	Upgrade the Change Guardian components.	◆ "Upgrading Policy Editor" on page 212 ◆ "Upgrading Change Guardian Agent for Windows" on page 212 ◆ Upgrading Change Guardian Agent for UNIX.

Upgrading a Traditional Installation

Ensure that NTP synchronized your computer time with the network time. Perform the upgrade in the following order:

1. Upgrading Change Guardian
2. Upgrading the Operating System

After completing the upgrade, perform the post upgrade configurations.

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.

To upgrade the Change Guardian Server in a traditional installation:

1 Back up your information using the `cgbackup_util.sh` script.

For information about using the backup utility, see Chapter 13, "Backing Up and Restoring Data," on page 197.

2 Download the latest installer from the Downloads website.

You must be a registered user to download patches. If you have not registered, click **Register** to create a user account in the patch download site.

3 Copy the installer file to a directory that has 0755 permissions.

NOTE: Trying to upgrade from any directory within `/root` fails because certain upgrade commands run as non-root user. Such commands cannot run if the installer is in the `/root` directory.

4 Log in as `root` to the Change Guardian server you want to upgrade.

5 Extract install files from the tar file:

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

6 Change to the directory where the install file was extracted.

7 Start the upgrade:

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

8 (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 the path must have 0755 permissions.

9 (Conditional) If NTP could not synchronize your computer time with the network time, make the required changes.

10 (Conditional) If your system does not meet the recommended disk space, make the required changes to the computer.

NOTE: The recommended disk space is for Change Guardian upgrade files. Allocate the recommended space in /, /var/opt, and /opt.

11 To proceed with a language of your choice, select the number next to the language.

12 If there are changes to the end user license agreement, read and accept the changes.

13 Specify yes to approve the upgrade.

The upgrade might take a few seconds to complete.

14 Validate and confirm the versions to be updated during the upgrade.

15 Verify that you can connect to the Change Guardian web interface by accessing the following URL:

https://*IP_Address_Change_Guardian_server*:8443

16 (Conditional) If your server was in FIPS mode prior to upgrade, import Elasticsearch certificate to FIPS keystore. For more information, see Importing Certificates to FIPS Keystore Database.

Based on your security requirement, perform the post upgrade configurations.

Upgrading the Operating System

If the Change Guardian server is running a version of an operating system that is not certified, some features might not function as expected. Upgrade to a supported operating system for a seamless experience.

To upgrade the operating system:

1 Log in as root to the machine running Change Guardian.

2 Stop the Change Guardian services:

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

3 (Conditional) If Change Guardian was in FIPS mode before the operating system upgrade, upgrade the NSS database:

```
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 the /etc/opt/novell/sentinel/3rdparty/nss directory:

```
cert9.db
key4.db
pkcs11.txt
```

4. Upgrade the operating system.
5. (Conditional) If you use Mozilla Network Security Services (NSS) 3.29 or later, install the two dependent RPM files:
   - `libfreebl3-hmac`
   - `libsoftokn3-hmac`
6. (Conditional) For RHEL 7.x, check whether there are any errors in the RPM database:

   ```
   rpm -qa --dbpath <installation_directory>/rpm | grep novell
   ```

   Example: `# rpm -qa --dbpath /custom/rpm | grep novell`
   - If there are any errors, fix the errors:

     ```
     rpm --rebuilddb --dbpath <installation_directory>/rpm
     ```

     For example: # rpm --rebuilddb --dbpath /custom/rpm
   - Recheck that there are no errors:

     ```
     rpm -qa --dbpath <installation_directory>/rpm | grep novell
     ```

NOTE: If the base operating system version changes, see "Upgrading Python" on page 218.

Upgrading the Appliance Installation

For information about appliance upgrade paths, see "Appliance Upgrading Paths" on page 243.

Ensure that NTP synchronized your computer time with the network time. To upgrade the Change Guardian appliance, complete the following step:

"Applying Updates" on page 208

After completing the upgrade, perform the post upgrade configurations.

Applying Updates

The following are the three methods in which you can apply updates:

- "Applying Updates By Using the Change Guardian Appliance Console" on page 208
- "Applying Updates Using Zypper" on page 209
- "Performing Offline Updates" on page 210

Applying Updates By Using the Change Guardian Appliance Console

Pre-requisites:

Download and run the utility `change_guardian_appliance_configuration_utility-<version>.tar.gz` from Change Guardian downloads page.

1. Register to the Change Guardian appliance update channel.

2 Get the Change Guardian and the operating system updates from the appliance update channel.

NOTE: Check whether the product and operating system repositories are available and are enabled. If the two repositories are not available, reregister the appliance.

---

3 Log in to the Change Guardian Appliance Console as `vaadmin` or `root` user using the following URL: `https://IP_Address_Change_Guardian_server:9443`.

4 Click **Online Update**.

NOTE: When you apply appliance patches on a Change Guardian appliance, you will see a few conflicts for OS patches. Ensure to select Solution 1 to perform deinstallation of packages to proceed with upgrade for the conflicts.

---

5 (Conditional) If you want to schedule online updates, click **Schedule** and select the frequency.

6 (Conditional) If you want to update manually, complete the following steps:

6a Click **Schedule > Manual**.

6b To view the list of available patches, click **Refresh**.

6c Select **Needed Patches** from the drop-down list and click **Update Now**.

6d Select **Needed Patches** from the drop-down list to ensure that there are no pending updates.

7 (Conditional) If you want to view the details of a patch, complete the following steps:

7a Select **Installed Patches** or **Needed Patches**.

7b Select the name of the patch and click **View Info**.

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

9 Install the operating system package updates:

```
zypper up
```

10 Restart the Change Guardian services:

```
rcsentinel start
```

NOTE: If you receive an error message during the restart, see "Applying Updates on Change Guardian Appliance Fails With an Error Message" on page 237 for troubleshooting steps.

---

11 Restart the Change Guardian server:

```
reboot
```

Applying Updates Using Zypper

Zypper is a command-line package manager that allows you to perform an interactive upgrade of the Change Guardian appliance.

Pre-requisites:

Download and run the utility `change_guardian_appliance_configuration_utility-<version>.tar.gz` from Change Guardian downloads page.

1 Register to the Change Guardian appliance update channel.

2 Get the Change Guardian and the operating system updates from the appliance update channel.

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

4 (Conditional) Check whether the product and operating system repositories are available and are enabled:

```
zypper lr
```

NOTE: If the two repositories are not available, reregister the appliance.

5 Check for available updates:

```
zypper lp
```

6 Run the following command:

```
zypper patch
```

This checks the installed packages and resolves any file conflicts.

7 Rerun the command to install appliance updates:

```
zypper patch
```

NOTE: When you apply appliance patches on a Change Guardian appliance, you will see a few conflicts for OS patches. Ensure to select Solution 1 to perform deinstallation of packages to proceed with upgrade for the conflicts.

8 Install the operating system updates:

```
zypper up
```

9 Restart the Change Guardian services:

```
rcsentinel start
```

NOTE: If you receive an error message during the restart, see “Applying Updates on Change Guardian Appliance Fails With an Error Message” on page 237 for troubleshooting steps.

10 Restart the Change Guardian appliance:

```
reboot
```

For more information about Zypper, see Zypper Cheat Sheet.

Performing Offline Updates

You can perform an update by using an offline ISO file under the following conditions:

- When there is no internet access and you are unable to register the appliance.
- When you prefer not to download the latest release available in the appliance download repository, but an earlier release. For more information, see Product Support Lifecycle.
- When the current version that you are running is incompatible with the latest version, download a version that is compatible and then upgrade it to the latest version. For more information, see Product Support Lifecycle.

While applying the patch, if you encounter registry/ repository issues, clear the registry and repository entries in your system.

To clean up the registration and repository details on the appliance:

- Take a backup of the files before clearing the registry entries and create a backup directory. For example: `mkdir /etc/zypp/backup`
- Copy the following registry files to the backup directory. For example:
  - cp /etc/zypp/credentials.d /etc/zypp/backup
  - cp /etc/zypp/repos.d/* /etc/zypp/backup
  - cp /etc/zypp/services.d/* /etc/zypp/backup
- Delete the following registry files:

  ```
  rm -fr /etc/zypp/credentials.d
  rm -fr /etc/zypp/repos.d/*
  rm -fr /etc/zypp/services.d/*
  ```

For more information, contact Technical Support.

Applying the ISO Patch

Pre-requisites:

- Download the migration file `change_guardian_appliance_configuration_utility-<version>.tar.gz` from Downloads website.
- Log in to the server as root.
- Extract the files:

  ```
  tar -zxvf change_guardian_appliance_configuration_utility-<version>.tar.gz
  ```
- Change to the directory where the file was extracted.
- Run the migration utility:

  ```
  ./cg<version>_appliance_configuration.sh
  ```
- Follow the instructions

To apply the patch:

1. Download the patch to a directory. For example: `<directoryname>/change_guardian_offline_appliance-<version>.iso`
2. Create a directory for mounting the CD using a command. For example: `mkdir -p /opt/trial`
3. Mount the patch CD locally using a command. For example:

   ```
   mount <directoryname>/change_guardian_offline_appliance-<version>.iso /opt/trial
   ```
4. Add the product and operating system repositories. For example:

   ```
   zypper ar -c -t plaindir "/opt/trial/product-repo" "<product repository>"
   ```

   ```
   zypper ar -c -t plaindir "/opt/trial/osupdate-repo" "<operating system repository>"
   ```
5. (Optional) Confirm if the repos are added successfully using the command: `zypper repos`

6 Check if the patches are bundled in the patch CD using the command: `zypper lp`

7 Run command `zypper patch`. This checks the installed packages and resolves any file conflicts.

8 Rerun the command to install appliance updates: `zypper patch`

> **NOTE:** When you apply appliance patches on a Change Guardian appliance, you will see a few conflicts for OS patches. Ensure to select Solution 1 to perform deinstallation of packages to proceed with upgrade for the conflicts.

9 Install the operating system updates: `zypper up`

10 Clean up the repositories list using the following command:

```
zypper rr "<product repository>"
zypper rr "<operating system repository>"
```

11 Start Change Guardian services before reboot: rcsentinel start

12 After the update is complete, reboot the machine using the command: `reboot`

Upgrading Components

- "Upgrading Policy Editor" on page 212
- "Upgrading Change Guardian Agent for Windows" on page 212
- "Upgrading Change Guardian Agent for UNIX" on page 213
- "Upgrading Change Guardian Event Collector Add-on" on page 213

Upgrading Policy Editor

The process of upgrading and installing the Policy Editor is the same. For more information, see "Installing Policy Editor" on page 39.

Upgrading Change Guardian Agent for Windows

You can upgrade Change Guardian Agent for Windows manually or by using Agent Manager. You can also roll back an update.

> **NOTE:** Ensure that the system on which Change Guardian for Windows is running has the latest patch of Microsoft Windows running.

> **NOTE:** The procedure 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. Do not rename the default `.msi` installer package. For more information, see "Manual Installation" on page 41.

To upgrade using Agent Manager:

1 From assets list, select the agent you want to upgrade.

You can select multiple assets if Agent Manager uses the same credentials to connect to them.

2. (Conditional) Provide login credentials to connect to the assets and click **Next**.

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

3. Click **Manage Installation > Upgrade Agents**.
4. Select the version of the agent you want to upgrade.
5. Click **Start Upgrade**.

Upgrading Change Guardian Agent for UNIX

You can upgrade Change Guardian Agent for UNIX by using Agent Manager.

To upgrade Change Guardian Agent for UNIX:

1. From the assets list, select the asset where you want to upgrade the agent.

   If you select multiple computers, you must use the same credentials in all computers.

2. Click **Manage Installation > Upgrade Agents**.
3. Select the version of the agent you want to upgrade.
4. Click **Start Upgrade**.

Upgrading Change Guardian Event Collector Add-on

NOTE: The upgrade to the newer version of Change Guardian Event Collector Add-on for Windows is currently not supported. To upgrade, uninstall the current version and install a newer version of the collector.

To upgrade Change Guardian Event Collector Add-on for Windows:

1. Open the directory where the existing collector add-on is located and run the installer to uninstall the collector.
2. Install the latest version of Change Guardian event collector. To see the detailed procedure of installation, see Installing Change Guardian Event Collector Add-on for Windows.

Applying Updates to Change Guardian Components

You can use Agent Manager to upload the agent packages or the Policy Editor patch. These packages deploy bug fixes and improvements made to Change Guardian Agent for Windows, Change Guardian Agent for UNIX, or Policy Editor.

To apply the patch:

1. Download the patch from the Downloads website.
2. Log in to Agent Manager.
3. Click **All Assets > Manage Installation > Upload Package**.

   This uploads the package to the Change Guardian server.

4 To upgrade agents or download Policy Editor, log in to Agent Manager on the machine running the agent or Policy Editor.

5 (Conditional) To upgrade Policy Editor, click **All Assets > Manage Installation > Download Package**, and then begin upgrade.

   For more information about upgrading, see Upgrade Policy Editor.

6 (Conditional) To upgrade agents, click **Manage Installation > Upgrade Agents**.

Post Upgrade Configuration

Verify that the following settings are complete:

- Adding License for Application
- Configuring LDAP
- Re-indexing Event Data Partition
- Importing Certificates to FIPS Keystore Database (if the Change Guardian server is running on FIPS mode)
- Updating the Keystore Password
- Setting the Polling Interval in Agent Manager
- Upgrading Python (if the base operating system changed during a traditional upgrade)

Configuring LDAP

If you want to use secure LDAP connections on the previously configured AD server, you have to edit the existing settings.

Change Guardian does not support AD servers that are configured with either IP address or FQDN, and does not support AD user name in the following format: `cn=users,dc=domain,dc=lab`. After upgrading Change Guardian, edit the pre-configured AD servers by specifying the domain name as the **Active Directory Server**. Similarly, modify the user name with an administrator or a user that has access to the domain.

To edit:

1 Open the following URL and click **CONFIGURATION > LDAP CONNECTIONS**:

   `https://<IP_Address_Change_Guardian_server>:<port_number>`

   The default port is 8443. You can use a custom port if Change Guardian was installed with custom configurations.

2 Select the desired servers and edit the settings.

For more information about configuring LDAP, see "Configuring LDAP for AD Browsing" on page 62.

Re-indexing Event Data Partition

If indexing libraries are upgraded during Change Guardian upgrade, the underlying data formats also get updated and the data cannot be searched. Therefore, all event data partitions in the system should be indexed so that it can be searched. If the partitions are not re-indexed after an upgrade, search results and reports shows inconsistent data.

NOTE: Perform the re-indexing steps if you have upgraded from Change Guardian 5.2 or 6.0.

Re-indexing is required only for the existing event data partitions and not for the new incoming events.

You can re-index using one or both methods:

- "Re-indexing Using the Web Console" on page 215
- "Re-Indexing in the Offline Mode" on page 215

Re-indexing Using the Web Console

1 Open the following URL: `https://<IP_Address_Change_Guardian_server>:<port_number>`

The default port is 8443. You can use a custom port if Change Guardian was installed with custom configurations.

2 Open ADMINISTRATION tab and click **Storage > Event Partition Administration**.

NOTE: You can also the Event Partition Administration page from the Change Guardian web console. Click the Event Partition Administration link in the warning message at the top of the page.

3 Select either **Primary Storage** or **Secondary Storage**, depending on the type of event partition that you want to re-index.

4 Select the event partitions to re-index, by clicking **Date Range**.

5 Click **Start Re-indexing**.

The approximate time required to complete the operation is displayed depending on the storage type and the event data time range selected.

After the re-indexing operation completes, all log files related to the operation are available in the following log file: `<installation_directory>/var/opt/novell/sentinel/log/reindex0.0.log`

Re-Indexing in the Offline Mode

You can also use a tool to re-index event data partition, in the offline mode. The tool uses minimal number of resources without affecting any of the existing processes. Re-indexing operation in the offline mode takes longer when compared to reindexing by using the online mode.

You can run the tool outside the Change Guardian server. However, you must copy the Java files and the Change Guardian libraries folder to the machine from which you want to run the re-indexing tool.

Before you proceed, ensure that you have the following information:

- The path to the folder where Java 1.8 is located. For a default installation, the path is:

  `<installation_directory>/opt/novell/sentinel/jre/bin/java`

- The path to folder where Change Guardian libraries are present. For a default installation, the path is:

  `<installation_directory>/opt/novell/sentinel/lib`

- The location of event data partitions. For a default installation, the path for primary partitions is:

  `<installation_directory>/var/opt/novell/sentinel/data/eventdata/events/`

To re-index:

1. Log in to the Change Guardian server as `root`.
2. Run the following command:

   ```
   <installation_directory>/opt/novell/sentinel/jdk/bin/java -cp /opt/
   novell/sentinel/lib/ccsapp-8.4.0.0-RELEASE.jar
   esecurity.ccs.comp.event.indexedlog.IndexedLogRebuild -forcerebuild
   <partition-directory>/<partition_ID>
   ```

   - `-forcerebuild` is an optional parameter. If this option is not specified, the tool creates a backup of index folder and temporary files, which occupies additional disk-space.
   - *<partition-directory>* refers to the path where all the partitions are present. You can add multiple IDs separated by space.
   - *<partition_ID>* refers to the ID of the partition in the following format: 0200428_6E1CCA35-4BD4-102D-91CD-000C2907C76D or 20200428_6E1CCA35-4BD4-102D-91CD-000C2907C76D_20200607

   If there are more than one partition, specify the IDs separated by space. You can also use the wild cards for ID such as, 202004*.

   For example, to re-index a single event data partition, specify the following command:

   ```
   <installation_directory>/opt/
   novell/sentinel/jdk/bin/java -cp /opt/novell/sentinel/lib/ccsapp-
   8.4.0.0-RELEASE.jar
   esecurity.ccs.comp.event.indexedlog.IndexedLogRebuild -forcerebuild /
   var/opt/novell/sentinel/data/eventdata/events/20200428_6E1CCA35-4BD4-
   102D-91CD-000C2907C76D
   ```

   For example, to re-index multiple event data partitions for April 2020, specify the following command:

   ```
   <installation_directory>/opt/
   novell/sentinel/jdk/bin/java -cp /opt/novell/sentinel/lib/ccsapp-
   8.4.0.0-RELEASE.jar
   esecurity.ccs.comp.event.indexedlog.IndexedLogRebuild -forcerebuild /
   var/opt/novell/sentinel/data/eventdata/events/202004*
   ```

Importing Certificates to FIPS Keystore Database

To import:

1. Change directory to `/opt/novell/sentinel/bin`, and run the following command:

   `./convert_to_fips.sh -i <path_to_certificate>` inserts the given certificate into the FIPS keystore database.
2. For example: `./convert_to_fips.sh -i <installation_directory>/opt/novell/sentinel/3rdparty/elasticsearch/config/http.pks`
3. Specify the password for the FIPS keystore database
4. Specify the certificate alias
5. You must restart the Sentinel server after inserting certificate. `Do you want to restart the Sentinel server now? yes/no [y]` => yes

Updating the Keystore Password

The `chg_keystore_pass.sh` script allows you to change the keystore passwords. As a security best practice, change the keystore passwords immediately after upgrading Change Guardian.

NOTE: Do 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 `root`.
2. Switch user to `novell`.
3. Go to the `/opt/novell/sentinel/bin` directory.
4. Run the `chg_keystore_pass.sh` script and follow the on-screen prompts to change the keystore passwords.

NOTE: When you upgrade Change Guardian to 5.1 or later and change the keystore database password with specific special characters, the following exception are displayed: “Failed to initialize Communicator”.

Setting the Polling Interval in Agent Manager

The heartbeat of Change Guardian Agent for Windows (displayed as Polling Interval) and Change Guardian Agent for UNIX (displayed as Heartbeat) determines the frequency at which Change Guardian server checks health of agents. It is the interval at which any policy changes on the server is synced to agents. If you have less than 500 agents and configured up to 15 policies per agent, consider setting **Polling Interval** to 15 minutes. If you have more than 500 agents or configured more than 15 policies per agent, consider setting the interval to 60 minutes. This ensures that there is no congestion of network traffic due to exchange of policy and agent health data at frequent intervals.

In Agent Manager, click **Manage Installation > Reconfigure**, and set the desired **Polling Interval**.

NOTE: This interval is referred to as Heartbeat in Policy Editor.

Upgrading Python

During a traditional Change Guardian upgrade, when the base operating system version changes, you must check the Python version after upgrading both Change Guardian and the operating system. Change Guardian requires a compatible version of Python library to function properly and to ensure that the Change Guardian agents are upgraded successfully.

For example, consider that the base operating system changes from RHEL 6.10 to RHEL 7.9. If running the `python –V` command at the RHEL 6.10 server prompt shows Python version is 2.6.x, then after upgrading the command shows 2.7.x on RHEL 7.9. Although the operating system is using Python 2.7.x, Python shared object file (`.so`) might be built on Python 2.6.x.

Prerequisite: Before planning to upgrade Python, check which Python version the `plpython2.so` file is built on:

```
ldd <installation_directory>/opt/novell/sentinel/3rdparty/postgresql/lib/
postgresql/plpython2.so
```

If the output is as below, it indicates that this `.so` file is based on Python 2.6.x and you must upgrade Python after upgrading both Change Guardian and the operating system.

```
libpython2.6.so.1.0 => /usr/lib64/libpython2.6.so.1.0
```

If the output is as below, it indicates the `.so` file is not linked to a Python version, and you must upgrade Python after upgrading both Change Guardian and the operating system.

```
libpython2.6.so.1.0 => not found
```

To upgrade Python:

1. Stop the Sentinel services:

   ```
   rcsentinel stop
   ```

2. Change to the directory where `plpython2.so` file is present

   ```
   cd <installation_directory>/opt/novell/sentinel/3rdparty/postgresql/
   lib/postgresql
   ```

3. Remove the existing `.so` file which is pointing to 2.6.x:

   ```
   rm plpython2.so
   ```

4. Extract the `Python 2.7.x.so` file, which is present in `<installation_directory>/opt/novell/sentinel/3rdparty/postgresql/lib/postgresql`

   ```
   tar zxf plpython2.7.so.tar.gz
   ```

5. Set `novell` user permission on the file

   ```
   chown novell:novell plpython2.so
   ```

6. Verify that the file is pointing to the correct Python version:

   ```
   ldd <installation_directory>/opt/novell/sentinel/3rdparty/postgresql/
   lib/postgresql/plpython2.so
   ```

7. Start the Sentinel services:

   ```
   rcsentinel start
   ```

Verifying the Upgrade

To verify if the upgrade was successful, perform any of the following:

- Ensure that the server is running:

  ```
  netstat -an | grep LISTEN | grep <port_number>
  ```

  The possible *port_number* are 8443, 9443, 8094, or 8082. For example, running the command with ports 8443 and 9443 provides the following outputs respectively:

  ```
  tcp6      0      0 :::8443    :::*   LISTEN

  tcp       0      0 :::9443    :::*   LISTEN
  ```

- Verify that the latest packages are installed:

  ```
  rpm -qa | grep -i ncg
  ```

  For example, running the command after upgrading to Change Guardian 5.2 displays the following output:

  ```
  ncgUtils-5.2.0.0-12.x86_64
  ncgContent-5.2.0.0-12.x86_64
  ncgPolicyRepository-5.2.0.0-12.x86_64
  ```

- Access the Change Guardian dashboard:

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

For troubleshooting tips, see "Issues Related to Upgrade" on page 235.

15 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.

Issues in Change Guardian Server

No trusted certificate / SSLHandshakeException after upgrading Change Guardian in FIPS mode

Issue: Alerts cannot be viewed in server0.0.logs if there are exceptions like `Root cause: No trusted certificate found (sun.security.validator.ValidatorException) javax.net.ssl.SSLHandshakeException: No trusted certificate found at sun.security.ssl.Alert.createSSLException(Alert.java:131)`

Workaround: Import `Elasticsearch` certificate to FIPS keystore. For more information, see Importing Certificates to FIPS Keystore Database.

Alert Rule Deployment Fails Due to Wrong IP Entry in the Host

Issue: When you install the Change Guardian server, the correlation engine takes the IP address from the host. This issue occurs because the IP address of the machine gets changed and is not updated in the host.

Workaround: Update the host entry and restart the Change Guardian server.

Unable to start nq_javos process after switching from legacy profile profile_iqc to profile_javos

Issue: When you switch from legacy profile (`profile_iqc`) to secure profile (`profile_javos`), Javos service does not start.

Workaround: Check the `/opt/netiq/cg/javos/javos.out` file for any errors. If you see any errors related to `/opt/netiq/cg/javos/javos.yml` file content missing, please check if the following lines are present in `/opt/netiq/cg/javos/javos.yml` file. If not, add the highlighted lines to the file. After updating the `/opt/netiq/cg/javos/javos.yml` file, restart the Javos service with the command: `/etc/init.d/nq_javos restart`.

cacheUpdateInterval: 60. Recommended value is 60, minimum value is 30.

Appenders:

type: file

currentLogFilename: `log/javos.log`

threshold: ALL

archive: true

archivedLogFilenamePattern: `log/javos-%i.log`

archivedFileCount: 5

maxFileSize: 2MB

timeZone: system

logFormat: `"%-5level [%date] [%t] %logger: %msg%n%rEx"`

Windows Policy Assignment Fails Due to IP Address Change in the Server

Issue: When the host name or IP address of the Change Guardian server is changed, the existing agents and CAM fail to communicate and the policy assignment too fails.

Workaround: Update the Event Destination with the new host name or IP address, For more information, see Change of IP and Host Name of the Change Guardian Server.

Firewall Status Shows 'Stopped' in Change Guardian Appliance Environments

Issue: The status of the `SuSEfirewall2` shows as "stopped" in the Change Guardian Appliance environments.

Workaround: Start the firewall and save the firewall configuration by using the command `#rcSuSEfirewall2 start` and `#chkconfig SuSEfirewall2_init on`.

Configuring Change Guardian Appliance to Boot Normally

Issue: Rebooting the Change Guardian Appliance in Hyper-V causes it to go into emergency mode. This issue occurs because the operating system modifies the disk UUID during installation.

Workaround: Install Change Guardian 5.1 appliance in Hyper-V and then upgrade to Change Guardian 6.0 appliance to resolve this issue. Alternately, you can update the UUID.

To update the UUID:

1. (Conditional) If the Change Guardian Appliance rebooted into emergency mode, login as `root`.
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. (Conditional) 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 15-1 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 (Conditional) To exit the emergency mode, reboot the virtual machine.

The SCSI disk partition UUIDs are detected correctly and the appliance boots normally.

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.

Cannot Connect to AD Hostname, Domain, or IP Address

Issue: The subject alternate name (SAN) in the AD certificate must exactly match the AD hostname, domain, or IP address to which you are trying to connect. If they do not match, the connection fails with an error message such as:

```
server0.0.log - CertificateException: No subject alternative DNS name
matching ip address/hostname/dns found.
```

Workaround: Regenerate the LDAP server certificate so that the SAN or the subject name of the certificate matches that of the LDAP server.

If you are unable to regenerate the LDAP server certificate, update `nq_ldap_expander` and `server.conf` files:

1. Open the `/etc/init.d/nq_ldap_expander` file.
2. Add the following text:

   ```
   -Dcom.sun.jndi.ldap.object.disableEndpointIdentification=true
   ```

   For example:

   ```
   RUNCMD="(cd ${PROCESS_BIN}; nohup  ${JAVA} -
   Dcom.sun.jndi.ldap.object.disableEndpointIdentification=true -jar ./
   ${DAEMON_FILE}.jar server ./${DAEMON_FILE}.yml > ${DAEMON_FILE}.out
   2>&1; rm ${PIDFILE}) &"
   ```
3. Open the `/etc/opt/novell/sentinel/config/server.conf` file.
4. Add the following text next to “`wrapper.java.additional.74=`”

   ```
   -Dcom.sun.jndi.ldap.object.disableEndpointIdentification=true
   ```

   For example:

   ```
   wrapper.java.additional.74=-
   Dcom.sun.jndi.ldap.object.disableEndpointIdentification=true
   ```
5. Go to `/opt/netiq/cg/scripts`.
6. Restart the services:

   ```
   ./cg_services.sh restart
   ```

Creating or Modifying an LDAP Connection in FIPS Mode Fails With Certificate Error

Issue: When you create or modify an LDAP connection (**CONFIGURATION > LDAP Connections**) in FIPS mode, and specify a previously uploaded SSL certificate, the LDAP Configuration page displays an error: “File already exists.” (`Defect 310249`)

Workaround: Delete the certificate manually and create the LDAP connection.

To delete:

1. List the certificates:

   ```
   certutil -L -d sql:/etc/opt/novell/sentinel/3rdparty/nss/
   ```

2 Delete the SSL certificate:

```
certutil -d sql:/etc/opt/novell/sentinel/3rdparty/nss/ -D -n
<certificate nickname>
```

Modifying the Certificate Validity Period

To modify the certificate validity period in Change Guardian server script and reconfigure agents:

1 Login to Change Guardian server as root and navigate to the following path:

`/opt/netiq/cgutils/bin/`

2 Edit the file `createClientCerts.sh` to change value of `CertNumDays` from 36500 to 3650 days. Save the changes.

3 **To view the certificate validity period changes:**

3a Updating the createClientCerts.sh file as in step 2 ensures that the validity is set to 3650 days for the fresh agent installations.

3b For the existing agents, you must reconfigure the agents. Login to Change Guardian Web UI and use the steps in "Reconfiguring the Agent" on page 62.

4 **(Conditional) To download the agent artifacts and certificates for fresh installations:**

4a For Change Guardian Agent for Windows follow the steps in "Installing Change Guardian Agent for Windows" on page 42.

4b For Change Guardian Agent for UNIX, follow the steps in "Installing Change Guardian Agent for UNIX" on page 52.

5 **(Conditional) Replacing the certificates for manual-deployed agents:**

Download and extract the `ChangeGuardianAgentCertificates_<hostname>.zip` file.

5a To replace certificate in the Change Agent for UNIX, copy the extracted `vigilent-agent-pk.pem`, `vigilent-agent-cert.pem` and `javosca-bundle.pem` to `/usr/netiq/cmnagent/codecs/vosSSLCodec/iqlsaca/certs/`.

5b To replace certificate in the Change Guardian agent for Windows, copy the extracted `vigilent-agent-pk.pem`, `vigilent-agent-cert.pem` and `javosca-bundle.pem` to `C:\Program Files (x86)\NetIQ\ChangeGuardianAgent\codecs\vosSSLCodec\iqlsaca\certs`.

5c Restart the agent services.

Issues in Change Guardian Interfaces

- "After Logging in to the Web Console, Opening ADMINISTRATION tab Displays Blank Page on Internet Explorer" on page 227
- "Unable to View Alerts in the Alerts Dashboard and Alert Views" on page 227
- "Cannot View Alerts with IPv6 Data in Alert Views" on page 227
- "Cannot Expand Grouped Events if Event Name Contains "Filter"" on page 227

After Logging in to the Web Console, Opening ADMINISTRATION tab Displays Blank Page on Internet Explorer

Issue: After logging in to the web console, clicking on **ADMINISTRATION** tab opens a blank page if Internet Security Level is set to High, and if the file download pop-up is blocked by the browser.

Workaround: Set the security level to Medium-high and then change to Custom level as follows:

To change the settings:

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.

Unable to View Alerts in the Alerts Dashboard and Alert Views

Issue: The Alert Dashboard and the charts in the alert view do not refresh or display new alerts. This issue could happen because of a corrupt alert index.

Workaround: Use the table in the alert view to see the newly generated alerts.

Cannot View Alerts with IPv6 Data in Alert Views

Issue: Change Guardian alert views do not display alerts that have IPv6 addresses in IP address fields. `(Defect 170317)`

Workaround: To view alerts with IPV6 addresses, perform the steps mentioned in NetIQ Knowledge base Article 7016555.

Cannot Expand Grouped Events if Event Name Contains “Filter”

Issue: In the Change Guardian dashboard, expanding grouped events fails with the following error message: `Data Loading Error`. The error occurs when the event name contains “filter”. `(Defect 172355)`

Workaround: Search events by name if it contains “filter”.

Issues Related to Events

- “Managed Events are Displayed as Unmanaged” on page 228
- ““Pathname Modified” Events in AWS IAM Does Not Display the Path Change” on page 228
- “Change Guardian Receives an Invalid Configuration Event” on page 228
- “Change Guardian is Unable to Receive Azure AD Events” on page 228
- “Source Name is Not Displayed When AD Events are Generated Using RDP” on page 229
- “Change Guardian Receives an Insufficient Access Permission Event” on page 229

Managed Events are Displayed as Unmanaged

Issue: When you create policies specifying managed users, events generated by such users might be wrongly displayed as unmanaged. This happens when a new user is added to AD and AD users are not synchronized with Change Guardian. Events generated by the newly added user is displayed as unmanaged events till the polling interval with AD has passed. `(Defect 313058)`

Workaround: Allow the polling interval with AD to pass so that events generated by the new users are displayed correctly as managed.

“Pathname Modified” Events in AWS IAM Does Not Display the Path Change

Issue: When AWS IAM generates “Pathname Modified” events for users and groups, Change Guardian displays the change in username and groupname, but does not display the change in path. `(Defect 172063)`

Workaround: None.

Change Guardian Receives an Invalid Configuration Event

Issue: Change Guardian receives Invalid Configuration event 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

Source Name is Not Displayed When AD Events are Generated Using RDP

Issue: Change Guardian Event Dashboard displays the source name as “N/A” or is blank when AD events are generated while logged in to the source machine using RDP. `(Defect 301102)`

Workaround: None.

Change Guardian Receives an Insufficient Access Permission Event

Issue: Change Guardian receives Insufficient Access Permission event 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 to receive events.

Cannot Generate Some Azure AD events in Change Guardian

Change Guardian cannot generate events from Azure Active Directory for the following events and attributes:

- Create Group Settings
- Update Group Settings
- Delete Group Settings
- Set group managed by
- Group Attributes
  - Is Membership Rule Locked

Change Guardian also does not support the following:

- Consolidating multiple events into a single event for Update user and Update group events
- Monitoring managed groups

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.

Change Guardian is not Receiving Events from Dell EMC

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:

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`

Change Guardian Server Does not Generate Events After Password Change

Issue: After you change the Change Guardian password, events are not generated because the REST dispatcher password is not updated in Policy Editor. `(Bug 1121890)`

Workaround: Enter the new password for the REST dispatcher by using Policy Editor, then restart the Change Guardian server:

```
rcsentinel restart
```

Events Dashboard Does not Display UNIX Events

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

Workaround: Verify if the spool file entry is frequently updated in the following directory:

```
/usr/netiq/vsau/local/spool/<unix_platform>AuditObject__singleton/
*.udetect_events
```

Change Guardian Server Does Generate Events When Write Permissions Are Modified

Issue: When you modify the write permission to rule group of a file on a UNIX system, Change Guardian fails to generate events for file monitoring.

Workaround: None.

Failed Events from Some Assets are Categorized with Severity 2

Issue: When authorized users perform actions that fail, such events are categorized with severity 2. This happens for events generated at AWS IAM, Dell EMC, Office 365, and Microsoft Exchange. `(Defect 165010)`

Workaround: Use appropriate filters to receive alerts from such assets.

Issues in Agent Manager

- "Deleting an Asset with Agent Manager Does Not Delete All Components" on page 231
- "Unable to Browse File Locations and AD Using Policy Editor File Browser" on page 231
- "Manually Uninstalling an Agent Does Not Remove the Version Details of an Agent" on page 232

Deleting an Asset with Agent Manager Does Not Delete All Components

Issue: If you delete an asset using Agent Manager, the Change Guardian Agent component is not deleted from the Installed Programs list in Windows. `(Defect 170281)`

Workaround: Uninstall the Change Guardian Agent component and use Agent Manager to delete the asset from Change Guardian. This removes all asset components completely.

Unable to Browse File Locations and AD 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.

Manually Uninstalling an Agent Does Not Remove the Version Details of an Agent

Issue: If you manually uninstall an agent, Agent Manager continues to display version details for the agent. (`Defect 170283`)

Workaround: In Agent Manager, select the agent in the 'All Assets' group and delete it.

Issues on Change Guardian Agent for Windows

- "Error Appears in VigilEntAgent_8094.log (ERROR [Minifilter_Collector]) for Windows Machine" on page 232
- "Installing Change Guardian Agent for Windows Fails with SMB Protocol Mismatch" on page 232
- "Collecting Agent Logs" on page 233
- "Change the Agent Package Version" on page 233

Error Appears in VigilEntAgent_8094.log (ERROR [Minifilter_Collector]) for Windows Machine

Issue: Windows Agent VigilEntAgent_8094.log shows the error `Minifilter_Collector`.

Workaround: Reconfigure the agent through Agent Manager to address these errors.

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.

Collecting Agent Logs

You can use Agent Manger to collect logs from Change Guardian Agent for Windows. For more information, see "Collecting Agent Logs" on page 234.

Change the Agent Package Version

Issue: You have a requirement to roll back to an older version of the agent package, but 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`.

Issues on Change Guardian Agent for UNIX

- "Unable to Connect to Port" on page 233
- "Unable to Run the Services" on page 233
- "Policies Are Not Applied to the Agent" on page 234
- "Events are not Generated After Configuring Change Guardian Agent for UNIX" on page 234
- "Cannot Browse User While Creating Policies" on page 234
- "Collecting Agent Logs" on page 234

Unable to Connect to Port

Issue: Change Guardian Agent for UNIX is not able to connect to port 8094.

Workaround: Check whether the port 8094 is running:

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

Unable to Run the Services

Issue: Change Guardian Agent for UNIX services are not running.

Workaround:

1. Check if the `detectd` and `auditd` services are running:

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

2. (Conditional) If the services are not running, restart the following services:

   2a Restart `vigilentagent` service:

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

   2b Go to the - `/usr/netiq/pssetup` directory and run the following command:

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

2c Restart `auditd` service:

```
service auditd restart
```

Policies Are Not Applied to the Agent

Issue: The policies are not applied to the Change Guardian Agent for UNIX after it is assigned using Policy Editor.

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

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

Events are not Generated After Configuring Change Guardian Agent for UNIX

Issue: Change Guardian Agent for UNIX fails to send events to the Change Guardian Server if the locale setting is incorrect. (`Bug 1102111`)

Workaround: Ensure that the following is set:

1. The path is set at the operating system: `SET_PERL_LIBPATH=1; ./etc/vsaunix.cfg`
2. The locale variables are added to the `/etc/profile` file:
   - `export LC_CTYPE=en_US.UTF-8`
   - `export LC_ALL=en_US.UTF-8`

Cannot Browse User While Creating Policies

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

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

To enter the data source paths:

1 (Conditional) If your operating system is 64-bit, in the registry `\HKLM\SOFTWARE\Wow6432Node\NetIQ\ChangeGuardianAgent\repositoryEnabled` set the `repositoryEnabled` flag to 1.

2 Restart the Change Guardian Agent for Windows.

Collecting Agent Logs

You can use Agent Manger to collect logs from Change Guardian 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.

Issues Related to Upgrade

- "Upgrade Fails with the Error Message "MongoDB authentication failed"" on page 235
- "When you update the OS, Packages that are Not Signed by Red Hat are Found" on page 236
- "Deploying Alert Rules Fail" on page 236
- "Change Guardian Configuration Fails after Appliance Installation Completes" on page 236
- "Cleaning Up Data From PostgreSQL When Migration Fails" on page 237
- "Exception After Changing Keystore Password with Specific Special Characters" on page 237
- "Applying Updates on Change Guardian Appliance Fails With an Error Message" on page 237

Upgrade Fails with the Error Message "MongoDB authentication failed"

Issue: The upgrade process fails when it is not able to authenticate the MongoDB database.

Workaround: Modify the Change Guardian `admin` user password.

To modify the password:

1. Shut down Change Guardian server

   ```
   rcsentinel stop
   ```

2. Run the configure.sh script from the /`opt/novell/sentinel/setup` directory:

   ```
   ./configure.sh
   ```

3. Specify 1 to perform a standard configuration of Change Guardian.
4. Specify 2 to create a new password and confirm the new password.

   The Change Guardian server starts.

5. (Conditional) If you are upgrading a Change Guardian appliance, perform the following steps:

   5a Remove the `migration.offset` file:

   ```
   rm -rf /var/opt/novell/sentinel/log/migration.offset
   ```

   5b Run the Change Guardian migration script:

   ```
   ./cg6000_appliance_configuration.sh
   ```

When you update the OS, Packages that are Not Signed by Red Hat are Found

Issue: When you upgrade supported RHEL Operating System from version 7.x to 8.x, a warning message appears for the CG packages that are not signed by Red Hat.

Workaround: Ignore the warning messages. Take a snapshot/ backup before upgrading the OS. You can delete the backup when the update is completed and the product functionality is working as expected or is intact.

Deploying Alert Rules Fail

Issue: Deploying an alert rule fails when you create, modify, or delete an alert rule after an upgrade. Although Deployment Status shows Success, the Alert Rule Deployment Status window displays an error that deployment has failed.

Workaround:

To resolve the issue:

1. Comment the IP address 127.0.0.2 in the `/etc/hosts` file.
2. Restart the Change Guardian server:

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

Change Guardian Configuration Fails after Appliance Installation Completes

Issue: After appliance installation, configuration of Change Guardian might fail to complete with the following error message:

```
Change Guardian configuration has failed. Check /var/opt/novell/sentinel/
log/config_cg_onboot.log.
```

In such a case Agent Manager and `javos` services might fail to start.

Workaround: Reconfigure Change Guardian.

To reconfigure Change Guardian:

1. Verify if Change Guardian service (8443) is running using the command:

   ```
   netstat -an | grep "8443" | grep "LISTEN"
   ```

2. (Conditional) If Change Guardian service (8443) is not running, start Change Guardian service (8443):

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

3. Reconfigure Change Guardian:

   ```
   /opt/novell/sentinel/setup/configure.sh
   ```

Cleaning Up Data From PostgreSQL When Migration Fails

Issue: Database migration to PostgreSQL fails.

Workaround: Delete the data that was partially moved to the PostgreSQL database.

To clear PostgreSQL:

1. Ensure that the PostgreSQL database is running.
2. Log in to the Change Guardian server as `root` and switch to `novell` user.
3. Go to the location where you have extracted the Change Guardian installer or the migration utility.
4. Delete the migrated data:

   ```
   ./db_migration_failure_cleanup.sh
   ```
5. (Conditional) If you are performing a traditional upgrading, upgrade Change Guardian.
6. (Conditional) If you are upgrading an appliance, run the appliance configuration utility.

Exception After Changing Keystore Password with Specific Special Characters

Issue: When you upgrade Change Guardian to 5.1 or later and change the keystore database password with specific special characters, the following exception are displayed: `Failed to initialize Communicator (Defect 172329)`

Workaround: None.

Applying Updates on Change Guardian Appliance Fails With an Error Message

Issue: When you restart the Change Guardian services during an appliance update, the following error messages might be displayed:

```
Exception in thread "main" java.lang.NoSuchMethodError: 
org.apache.http.impl.client.HttpClientBuilder.setSSLHostnameVerifier(Ljava
x/net/ssl/HostnameVerifier;)Lorg/apache/http/impl/client/
HttpClientBuilder;
  at 
esecurity.ccs.comp.event.visualization.ESRestUtil.<init>(ESRestUtil.java:1
12)
  at 
esecurity.ccs.comp.event.visualization.ESRestUtil.getInstance(ESRestUtil.j
ava:121)
  at 
esecurity.ccs.comp.event.visualization.ESRestUtil.main(ESRestUtil.java:136
)
```

Workaround: Perform the following steps:

1. Switch to the directory `/<installation-path>/opt/novell/sentinel/bin/`
2. Open the `elasticsearch.sh` file.

3 Change `LIB_LOCATION="${ESEC_HOME}/lib/*:. "` to `LIB_LOCATION="${ESEC_HOME}/lib/ccsapp*.jar "`.

4 Open the following files and perform step 3:

- `create_kibana_index_pattern.sh`
- `elasticsearch_index_template.sh`
- `elasticsearchRestClient.sh`
- `load_kibana_data.sh`
- `reSyncAlert.sh`

Issues on Federated Servers

If you have enabled data federation in your environment, review the following issues:

- "Permission Denied" on page 238
- "Connection Down" on page 238
- "Unable to View Raw Data" on page 239
- "Problems While Adding Data Source" on page 239
- "Some Events Are Only Visible from the Local System" on page 239
- "Different Users Get Different Results" on page 239
- "Cannot Set the Administrator Role as the Search Proxy Role" on page 239
- "Error Logs" on page 239

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 "Allowing Access to an Authorized Requestor Server" on page 147.
- 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. For more information, see "Allowing Access to an Authorized Requestor Server" on page 147.
- The role that you used to connect 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 might have 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 the 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. This happens if 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 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.

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 Administrator Role as the Search Proxy Role

This is by design, for security reasons. Because the data viewing rights for the administrator are unrestricted, it is not desirable to allow the administrator 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
```

Troubleshooting Notes

Change Guardian Server Issues

- Server unresponsive
- Authentication failures
- Event/ Alert migration failures
- Database migration failures
- LDAP Authentication issues, etc.

How to Troubleshoot?

1. Check status of ports:
   - Webserver/ 8443
   - PostgreSQL/5432
2. Check Firewall status
3. Check whether the product RPMS are installed and upgraded successfully
4. Logs to be collected:
   - `/var/opt/novell/sentinel/log`

Change Guardian Agent Issues

- Agent deployment/ upgrade through AMS failures
- Heartbeat, Agent health issues
- Policy Assignment and Event generation failures, etc.

How to Troubleshoot?

1. Check status of ports in server
   - Agent Manager/8082
   - JAVOS/8094
   - LDAPExpander/8079
2. Check whether the install and upgrade is completed successfully
3. Logs to be collected:
   - In server machine:
     - AMS logs: `/opt/netiq/ams/ams/log/ams.log ; /opt/netiq/ams/assets/log/assets.log`
     - JAVOS: `/opt/netiq/cg/javos/log/javos.log`
     - Certificate setup logs: `/opt/netiq/cgutils/certs/cert-setup.log`

- In Agent machines:
  - Agent logs: `C:\ProgramData\NetIQ\ChangeGuardianAgent\`
  - CAM logs: `C:\ProgramData\NetIQ\ClientAgentManager\`

Change Guardian CAF UI Issues

- CAF/ 9443 UI loading issues
- Channel Registration issues, etc.

How to Troubleshoot?

1. Check status of ports in server:
   - CAF/ 9443
2. Check the status of services:
   - `systemctl status vabase-datamodel.service vabase-jetty.service vabase.service`
3. Logs to be collected:
   - In server machine
     - `/var/opt/novell/jetty/logs/jetty.stderrout.out`
     - `/var/opt/novell/datamodel-service/logs/datamodel.stderrout.out`

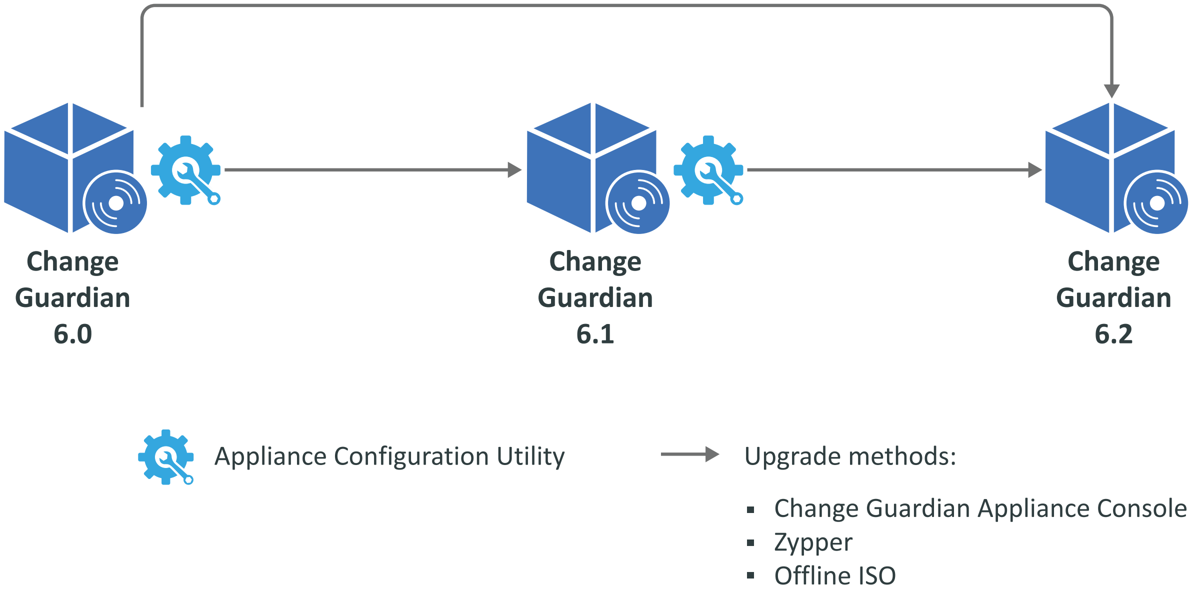
A Appendices

This chapter provides information about the following sections:

- "Appliance Upgrading Paths" on page 243
- "Uninstalling Change Guardian" on page 244
- "Expanding Disk Space in Hyper-V Virtual Machine" on page 247

Appliance Upgrading Paths

The following diagram illustrates the upgrade paths available for Change Guardian appliance:



Review the following to understand the upgrade paths:

- Change Guardian 6.2 supports appliance upgrade in ISO, OVF, and VHD formats.

  You must have applied the channel updates to upgrade from Change Guardian 6.0 or later. The channel now lists the Change Guardian 6.2 updates.
- Upgrade to Change Guardian 6.2 from Change Guardian 6.0 or 6.1.
- You can upgrade to a higher version using either of the following methods:
  - Change Guardian Appliance Console
  - Zypper
  - Offline ISO

Uninstalling Change Guardian

Checklist to Uninstall

Use the following checklist to uninstall Change Guardian:

- Uninstall the following components before you uninstall Change Guardian:
    - Change Guardian Agent for Windows and Change Guardian Agent for UNIX using Agent Manager
    - Policy Editor
- Complete the tasks after uninstalling to verify that Change Guardian is uninstalled
- Uninstall agents before uninstalling Change Guardian and the components

Task	See
Uninstall the components	“Uninstalling Change Guardian Event Collector Addon for Windows Agent” on page 244 “Uninstalling Change Guardian Agent for Windows” on page 245 “Uninstalling Change Guardian Agent for UNIX” on page 245 “Uninstalling Policy Editor” on page 246
Uninstall Change Guardian	“Uninstalling Change Guardian” on page 246
Perform the post-uninstall steps	“Tasks After Uninstalling” on page 246

Uninstalling Change Guardian Event Collector Addon for Windows Agent

To uninstall, open the Change Guardian Event Collector Addon for Windows Agent application.

Uninstalling Change Guardian Agent for Windows

Ensure that you have removed assets using Agent Manager.

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

- "Uninstalling Remotely" on page 245
- "Uninstalling Manually" on page 245

Uninstalling Remotely

1. Login to Change Guardian web console and navigate to **Agents**.
2. Select the assets from which you want to uninstall the agent.
3. Select **Manage Installation > Uninstall Agents**.
4. Click **Start Uninstall**.

Uninstalling Manually

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 Change Guardian Agent for UNIX

You can uninstall the Change Guardian Agent for UNIX in the following ways:

- "Uninstalling Remotely" on page 245
- "Uninstalling Manually" on page 245
- "Verifying Uninstall" on page 246

Uninstalling Remotely

To uninstall:

1. Select the assets from which you want to uninstall the agent.
2. Select **Manage Installation > Uninstall Agents**.
3. Click **Start Uninstall**.

To verify that you have successfully uninstalled, navigate to respective asset. Ensure that the asset is not listed in the assets list.

Uninstalling Manually

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

```
./uninstall.sh
```

Verifying Uninstall

Verify that you have successfully uninstalled, by performing the following:

- Check if all the components are uninstalled

  Run vi command on /etc/vsaunix.cfg configuration file to check if the parameter `CGU_INSTALLED` is n
- Check that none of the services are running by navigating to the /usr/sbin folder
- Check if the folder structure is deleted
- Check if assets that are uninstalled are not listed in the assets list

Uninstalling Policy Editor

NOTE: Before uninstalling Policy Editor, ensure agent/agent groups have been uninstalled.

To uninstall:

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

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**.

Tasks After Uninstalling

After you uninstall Change Guardian server:

- Reboot the computer to clear the cache files
- To ensure that the services are not running, run the following commands:

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

  NOTE: If the services are still running, reinstalling the Change Guardian server will fail with errors or exceptions. Rebooting the machine terminates any services that are running from the previous installation.
- Ensure that there are no files or system settings remaining from the previous installation

Expanding Disk Space in Hyper-V Virtual Machine

Prerequisite: Ensure that the current disk has the required space to expand by running the `fdisk -l` command at the Change Guardian appliance prompt.

NOTE: You can expand the partition if there are less than four primary partitions. However, if there are four primary partitions, add a new virtual disk to the virtual machine and expand the logical volume.

To expand the disk space:

1 Expand the disk space:

- **1a** Log in to the Hyper-V server and power off the virtual machine where you installed Change Guardian appliance.
- **1b** Right-click the virtual machine and click **Settings**.
- **1c** Under **IDE Controller**, click **Hard Drive**.
- **1d** Select **Virtual hard disk**, and click **Edit**.

  The Edit Virtual Hard Disk Wizard opens.
- **1e** In Locate Virtual Hard Disk, click **Next**.
- **1f** In Choose Action, Click **Expand > Next**.
- **1g** In Configure Disk, specify the disk size, and click **Next > Finish**.
- **1h** Turn the machine on.

2 Verify that the disk space has increased by running the following at the appliance prompt:

```
fdisk -l
```

3 Create a partition:

- **3a** Run the disk partitioning utility:

  ```
  fdisk <partition_name>
  ```

  For example, fdisk `/dev/sda`.
- **3b** To create a new partition, specify ‘n’.
- **3c** To create a primary partition, specify ‘p’.
- **3d** Specify the desired partition number.
- **3e** When prompted for the first and last sectors, press Enter.

4 Change the partition type:

- **4a** To change the partition type, specify ‘`t`’.
- **4b** Specify the partition number you had mentioned.
- **4c** Specify the Hex code as 8e.

5 To write the partition to the disk, specify ‘`w`’.

6 Scan for the newly created partition:

```
partprobe -s
```

The new partition number is listed in the output.

7 Verify that the partition is created:

```
fdisk -l
```

The details of the new partition and logical volumes are displayed. For example, the new partition is `/dev/sda3`. Make a note of the logical volume path to use in a later step. For example the path is `/dev/mapper/systemVG-LVvar_opt`.

8 Expand the logical volume with the new partition:

- **8a** Create a physical volume by replacing newly created partition:

  ```
  pvcreate <partition_name>
  ```

  For example, the command is: `pvcreate /dev/sda3`

- **8b** Find out the volume group name:

  ```
  vgdisplay
  ```

  For example, the volume group is displayed as `VG Name      volume_group1`.

- **8c** Expand the volume group:

  ```
  vgextend <volume_group_name> <partition_name>
  ```

  For example, the command is `vgextend volume_group1 /dev/sda3`.

- **8d** Check the newly added physical volume and the usable space:

  ```
  pvscan
  ```

- **8e** Expand the logical volume:

  ```
  lvextend <logical_volume_path> <partition_name>
  ```

  For example, the command is `lvextend /dev/mapper/systemVG-LVvar_opt /dev/sda3`.

- **8f** To use the newly created space, resize the file system to the logical volume:

  ```
  resize2fs <logical_volume_path>
  ```

  For example, the command is `resize2fs /dev/mapper/systemVG-LVvar_opt`.

- **8g** Display the total space and available space on the file system:

  ```
  df -h
  ```