User Guide

Change Guardian™

May 2018

Legal Notice

Contents

About this Book and the Library

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

Intended Audience

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

Other Information in the Library

The library provides the following information resources:

Help

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

Release Notes

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

1 Getting Started

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

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

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

This section provides information about the following:

What is Change Guardian?

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

To combat an increasingly sophisticated threat landscape and complex computing environment driven by such technologies as BYOD, mobility and cloud, organizations must take a layered and integrated approach to defend their critical systems and sensitive data.

Change Guardian provides the following protection measures:

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

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

- Centrally recording and auditing changes

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

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

Introduction to the Change Guardian Interface

There are different tools to help you take advantage of all of the features Change Guardian has to offer. You must have necessary permissions to access the following tools:

- **Threat Response Dashboard**: The Threat Response Dashboard is the main user interface for viewing and triaging alerts. Any user with permission to manage alerts can use the Threat Response Dashboard.

  NOTE: Users who wish to access the Change Guardian Main interface, or do not have permission to view or manage alerts on the Threat Response Dashboard, can click Change Guardian Main in the left side navigation to access the Change Guardian interface.

- **Change Guardian Main Interface**: The Change Guardian Main interface is the main user interface for viewing and interacting with Change Guardian data.

Accessing the Threat Response Dashboard

1. Launch a supported web browser.
2. Specify the URL of the Threat Response Dashboard:

   `https://<IP_Address_Change_Guardian_server:8443>`

   Where *8443* is the default port for the Change Guardian server.
3. Log in as a user with permissions to access the dashboard.

Accessing the Change Guardian Main Interface

If you are using the Threat Response Dashboard, click **Change Guardian Main**.

To access the Change Guardian Main interface through a browser:

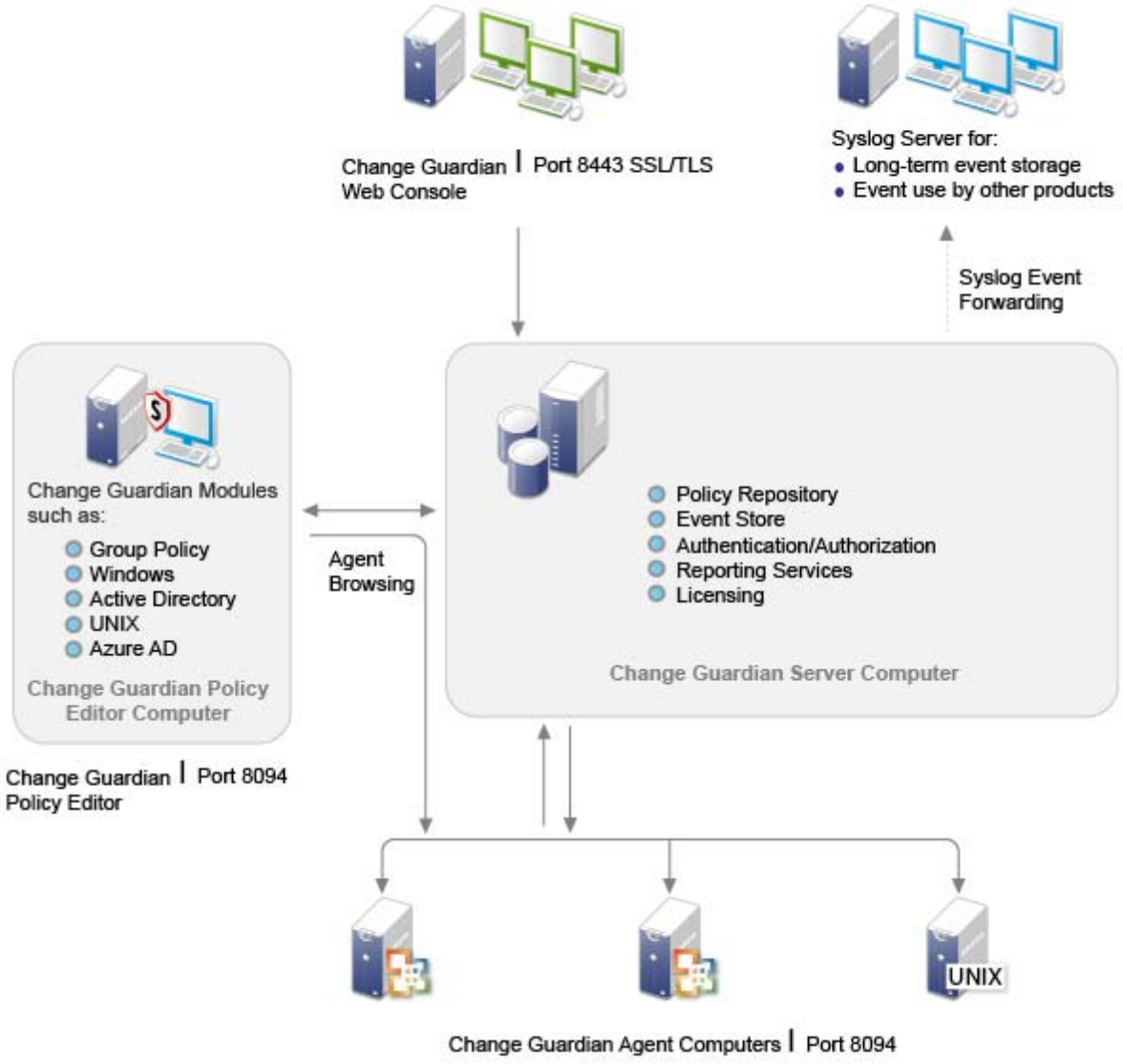
1. Launch a supported web browser.
2. Specify the URL of the Change Guardian Main interface:

   `https://<IIP_Address_Change_Guardian_server:8443>/sentinel/views/main.html`

   Where *8443* is the default port for the Change Guardian server.
3. Log in as a user with permissions to access the desired feature.

Understanding Change Guardian Components

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



Change Guardian includes the following major components:

Change Guardian Policy Editor

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

Change Guardian server

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

Change Guardian Main

A web console that allows you to monitor security event details that pinpoint the who, what, when, where, and authorization status of a change or activity, including before and after details of the change.

Agent Manager

A web console that provides a central location from where you can manage your agents, organize your assets in groups, and remotely install and update agents on assets. It helps you maintain your environment by keeping track of agents that are not communicating and allows you to either fix the agent or remove it from your environment.

Agents

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

Interoperability of Directory and Resource Administrator With Change Guardian For Privileged Monitoring

Change Guardian provides enhanced user monitoring in conjunction with Directory and Resource Administrator (DRA). Together they provide an integrated solution to control, manage, and monitor the Active Directory environment.

For example, when you use DRA to make changes to Active Directory, and you create a user from the **Create User** wizard in DRA, the Change Guardian server gets notified and the web console displays the actual user name of the user who logged in to DRA to make Active Directory changes.

Change Guardian enriches the event with an initiator application identifier, which helps you to view and filter the events generated by DRA. Change Guardian also populates DRA Transaction ID into the Change Guardian <event fields > <mention the field name after it is finalised>.

By monitoring activity in Active Directory, Change Guardian can detect if users are bypassing DRA and making changes to Active Directory that are not compliant with the policies defined in DRA.

Change Guardian displays the actual user name for the following specific set of actions performed using DRA in Active Directory:

- User account created
- User account modified
- User account unlocked
- User account enabled
- User account disabled
- Active Directory (AD) object created
- Active Directory (AD) object modified
- Computer account created
- Computer account modified
- Computer account enabled
- Computer account disabled
- Contact created
- Contact modified
- Group created
- Group modified

- Organizational Unit (OU) added
- Organizational Unit (OU) modified

Default Ports

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

Component	Ports	Direction	Required /Optional	Description
Policy Editor Console	8443	Outbound	Required	Connects to the Change Guardian server for the following actions: ◆ remote object browsing to Windows-based monitored assets ◆ configuring email in Change Guardian or Sentinel ◆ updating policies to the Change Guardian server
	2620	Outbound	Optional	Allows remote object browsing to UNIX-based monitored assets.
	389 or 636	Outbound	Optional	Allows remote object browsing to Active Directory.
Change Guardian server	8094	Inbound	Required	Allows the Change Guardian server to accept connections from agents that retrieve their assigned monitoring policies.
	8443	Inbound	Required	Allows the Change Guardian server to receive events from monitored assets. **NOTE:** This port might not be needed if you are sending events from monitored assets to an alternate destination.
	389 or 636	Outbound	Required	Enables the LDAP authentication and the expansion of Active Directory groups. The port initiates a connection to the LDAP server.
	25	Outbound	Optional	Default email port. This port may be different based on the specific email implementation.
JAVOS	8094	inbound	Required	Allows the JAVOS service to accept connections from agents that are retrieving their assigned monitoring policies.
	9094	Inbound (loopback)	Required	Allows the Change Guardian server to call JAVOS on this port to signal/reset the event destination cache.
	9095	Inbound (loopback)	Optional	Allows users to see runtime metrics and active threads.
Active Directory Accounts/ LDAP Expander	8088	Inbound (loopback)	Required	Allows the Change Guardian server to retrieve information about Active Directory accounts.
	8089	Inbound (loopback)	Optional	Allows users to see runtime metrics and active threads.

Component	Ports	Direction	Required /Optional	Description
Windows Monitoring Agents	8094	Outbound	Required	Allows the agent to connect to the Change Guardian server to retrieve assigned monitoring policies.
	8094	Inbound	Optional	Allows the Policy Editor to connect to the agent to browse objects on the monitored asset.
	8443	Outbound	Required	Allows the agent to connect to the Change Guardian server or Sentinel to send events.
UNIX Monitoring Agents	8094	Outbound	Required	Allows the agent to connect to the Change Guardian server to retrieve assigned monitoring policies.
	2620	Inbound	Optional	Allows the Policy Editor to connect to the agent to browse objects on the monitored asset.
	8443	Outbound	Required	Allows the agent to connect to the Change Guardian server or Sentinel to send events.
UNIX Agent Manager	2620	Outbound	Required	Allows the UNIX Agent Manager to connect to a UNIX agent to get status and diagnostic information.
	2222	Outbound	Required	Allows the UNIX Agent Manager client to connect with the UNIX Agent Manager server.
	22	Outbound	One of these is required.	(SSH) UNIX Agent Manager requires SSH+SFTP or Telnet+FTP access to computers targeted for remote agent deployment.
	21/23	Outbound		(Telnet/FTP) UNIX Agent Manager requires SSH+SFTP or Telnet+FTP access to computers targeted for remote agent deployment.
Agent Manager	8082	Inbound	Required	Allows the agent to communicate with the Agent Manager.
	445	Outbound	Required	Allows the Agent Manager to deploy agents to Windows computers.

Implementation Checklist

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

If you are upgrading from a previous version of Change Guardian, do not use this checklist. For information about upgrading, see Chapter 20, “Upgrading Change Guardian,” on page 153.

	Checklist Items
❑	If you have purchased Change Guardian, ensure that you have the following license keys: ◆ Change Guardian server ◆ Change Guardian Module Keys ◆ NCC channel registration codes (only for appliance installations) If you have not yet purchased Change Guardian, you may use the 60-day built-in trial license. For more information about licensing, see Chapter 2, “Understanding License Information,” on page 19. Contact your Sales Associate for further assistance.

	Checklist Items
❑	Determine whether you want to perform a traditional or appliance installation of the Change Guardian server. For more information, see Chapter 4, “Installing the Change Guardian server,” on page 29. ◆ If you want to perform a traditional installation, see “Traditional Change Guardian server Installation” on page 29. ◆ If you want to perform an appliance installation, see “Appliance Change Guardian server Installation” on page 31.
❑	Ensure the Change Guardian server is up and running by issuing the following command: `netstat -an | grep LISTEN | grep 8443`
❑	Ensure that the following line is not commented in the `/etc/hosts` file: `127.0.0.1 localhost`
❑	Synchronize the time on your Change Guardian server and monitored computers by using the Network Time Protocol (NTP).
❑	Verify whether the Change Guardian web console can connect to the server by specifying the following URL in your web browser: `https://`*IP_Address_Change_Guardian_server*`:8443`
❑	Install the Change Guardian Policy Editor. For more information, see “Installing the Policy Editor” on page 39.
❑	(Conditional) If you want to monitor events on UNIX computers, you can deploy and configure the Security Agent for UNIX using the following: ◆ UNIX Agent Manager (UAM) ◆ Change Guardian Agent Manager (CG AM) For more information, see *Security Agent for UNIX Configuration and Installation Guide*.
❑	(Conditional) If you want to monitor events on Windows computers, install the Windows agent. For more information, see Chapter 5, “Installing the Change Guardian Components,” on page 39.

Meeting System Requirements

A Change Guardian implementation can vary based on the needs of your IT environment, so you should contact Consulting Services or any of the Change Guardian partners prior to finalizing the Change Guardian architecture for your environment.

For information about the recommended hardware, supported operating systems, appliance platforms, and browsers, see the Change Guardian Technical Information website.

2 Understanding License Information

Change Guardian comprises a broad spectrum of functionality, which caters to various needs of its many customers. You can choose a licensing model that fulfills your needs.

Change Guardian licensing is described in relation to Change Guardian Instances, each of which requires a dedicated license per organization for the modules being monitored by Change Guardian. A Change Guardian Instance will typically consist of the following:

- At least one Change Guardian server
- One or more Change Guardian Agents
- A licensed count of monitored modules.

  The following is the list of Modules

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

The following are the types of Change Guardian licenses:

- “Evaluation Licenses” on page 19
- “Enterprise Licenses” on page 20
- “Adding a License Key” on page 20

Evaluation Licenses

The default evaluation license allows you to use all the features of Change Guardian for a 60-days evaluation period with unlimited EPS subject to the capacity of your hardware.

When you install Change Guardian server, you will receive evaluation licenses for all the modules for an evaluation period of 60-days.

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

After you upgrade to an enterprise license, Change Guardian restores all functionality. To prevent any interruption in functionality, you must upgrade the system with an enterprise license before the evaluation license expires.

Enterprise Licenses

When you purchase Change Guardian, you receive a license key through the customer portal for the Change Guardian server and all the modules. Depending on the license you purchase, your license key enables features, data collection rates, and event sources. There might be additional license terms that are not enforced by the license key, therefore read your license agreement carefully.

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

You can add the enterprise license key either during the installation or any time thereafter. To add the license key, see “Adding a License Key”.

Adding a License Key

You can add a license key when installing Change Guardian. This section provides information about adding the license key after the Change Guardian installation.

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

You can add a license key either by using the Change Guardian Main interface or through the command line.

Adding a License Key By Using the Change Guardian Main Interface

1. From Change Guardian main, click **About** > **Licenses**.
2. In the Licenses section, click **Add License**.
3. Specify the license key in the **Key** field. After you specify the license, the following information is displayed in the Preview section:

   Features: The features that are available with the license.

   Hostname: This field is for internal Novell use only.

   Serial: This field is for internal Novell use only.

   EPS: Event rate built into the license key. Beyond this rate, Change Guardian generates warnings but will continue to collect data.

   Expires: Expiry date of the license. You must specify a valid license key before the expiry date to prevent an interruption in functionality.
4. Click **Save**.

Adding a License Key through the Command Line

If you are using the Change Guardian traditional installation, you can add the license through the command line by using the `softwarekey.sh` script.

1. Log in to the Change Guardian server as `root`.
2. Change to the `/opt/novell/Change Guardian/bin` directory.

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

```
su novell
```

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

```
./softwarekey.sh
```

5 Enter 1 to insert the license key.

6 Specify the license key, then press Enter.

3 Security Considerations

This section provides information on how to securely maintain your Change Guardian server.

Basic Security Considerations

Change Guardian has undergone security hardening before being released. This section describes some of the hardening mechanisms used in Change Guardian.

Traditional Installation

- All unnecessary ports are turned off.
- Whenever possible, a service port listens 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.
- 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

In addition to the points mentioned in “Traditional Installation” on page 23, the appliance has undergone the following additional 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.

Network Communication Options

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

Using TLS for Communication

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

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

TLS 1.0 is not disabled by default in upgrade installations of the Change Guardian server, agents, and Policy Editor components in order to preserve backward compatibility with components that might not be upgraded yet. Once you upgrade all the components to the latest released versions, you can disable TLS 1.0. For more information, see Prerequisites.

The Change Guardian server, agents, and Policy Editor components allow TLSv1.0 for communication. To improve the security posture and to prevent known vulnerabilities, you can disable TLSv1.0.

Prerequisites

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

- Install curl-openssl1 on SLES 11 SP4 before disabling the TLS 1.0 protocol on the Change Guardian server. For information about the RPM prerequisites, see "Traditional Change Guardian server Installation" on page 29.
- Upgrade Windows agents to 5.0 or later.
- Upgrade Security Agent for UNIX to 7.5.1 or later.
- Ensure that TLS 1.1 or a higher version is enabled for the SMTP server configured in Policy Editor.
- Ensure that you have Microsoft .NET Framework 4.5 or later.

Disabling TLS 1.0

Perform the following steps on the Change Guardian server:

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

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

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

   When TLSv1 is included in the list of disabled algorithms, it forces the use of TLS 1.1 or above.

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

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

Enabling TLS 1.0

By default, TLS1.0 is disabled for new installations. You can enable the TLS1.0 protocol if you are required to integrate Change Guardian with components that do not have TLS 1.1 or higher enabled. For example: Security Agent for UNIX prior to 7.5.1 or an SMTP server using only TLS 1.0.

NOTE: You mus not enable TLS1.0, unless you want to ensure compatibility between the agents which support TLS1.0 and the Change Guardian server.

Perform the following steps on the Change Guardian server:

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

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

   After: `jdk.tls.disabledAlgorithms=SSLv3, RC4, MD5withRSA, DH keySize < 768`
4. Run the following command to restart the Change Guardian server:

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

Disabling 3DES Ciphers

The 3DES ciphers are enabled on new installations and upgrade installations by default. You can disable the 3DES ciphers for additional security and to reduce known vulnerabilities.

Perform the following steps on the Change Guardian server to disable 3DES ciphers:

1. Log in as the `novell` user.
2. Edit the `/etc/opt/novell/sentinel/3rdparty/jetty/jetty-ssl.xml` file.
3. Add the `SSL_RSA_WITH_3DES_EDE_CBC_SHA` cipher to the list of excluded ciphers.

   ```
   <Set name="ExcludeCipherSuites">
   <Array type="java.lang.String">
     ......
     .......
     <Item>SSL_RSA_WITH_3DES_EDE_CBC_SHA</Item>
   </Array>
   ```
4. Run the following command to restart the Change Guardian services:

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

Secure Communication Profile

You must perform this procedure after upgrading all the components to the latest released versions.

If you have upgraded your Change Guardian server to 5.0, you must perform the following procedure to ensure that the most secure security communication profile is enabled. You must switch communication profiles if you want Change Guardian to be PCI compliant.

IMPORTANT: If you use UAM to install or upgrade Security Agent for UNIX, you must use profile_iqc. You must not switch the secure communication profile to profile_javos.

In case you want to use profile_javos, you must upgrade all the existing agents using CG AM only, before you switch the secure communication profile to profile_javos. After switching to profile_javos, you must perform any installations and upgrades only via CG AM.

You should not perform this procedure if you have Secure Configuration Manager also installed along with Change Guardian in the same environment, because the SCM Core registration fails when you switch the security communication profile. For more information on how to register SCM, see Registering SCM in *Security Agent for UNIX documentation*.

Prerequisites:

Perform this procedure after upgrading all the components to the following minimum versions:

- Change Guardian 5.0 (including all agents and Policy Editor clients).
- Security Agent 7.5.1.

Perform the following steps:

1. Log in as a `root` user.
2. Run the following command to verify whether the profile_iqc is active: `/opt/netiq/cg/javos/bin # ./javos_cert_setup.sh --show`

   The following success message is displayed:

   ```
   Enabled profile: profile_iqc
   ```

3. Run the following command to switch profile_iqc to profile_javos: `/opt/netiq/cg/javos/bin # ./javos_cert_setup.sh --enable --profile=profile_javos`.
4. Run the following command to verify that profile_javos is active: `/opt/netiq/cg/javos/bin # ./javos_cert_setup.sh --show`.

   The following success message is displayed:

   ```
   Enabled profile: profile_javos
   ```

5. (Conditional) If Change Guardian server is in FIPS mode, you should re-run the `convert_to_fips.sh` script.

Applying Updates for Security Vulnerabilities in Embedded Third-Party Products

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

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

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

4 Installing the Change Guardian server

This chapter guides you through installing the Change Guardian server. The Change Guardian server provides policy and event storage and communication with monitored computers and systems to which you want to forward events. For more information, see “Understanding Change Guardian Components” on page 12.

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

Planning for Change Guardian server Installation

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

A Change Guardian implementation can vary based on the needs of your IT environment, so you should contact Consulting Services or any of the Sentinel partners prior to finalizing the Sentinel architecture for your environment.

Change Guardian offers enhanced protection against security threats and compliance with United States federal government standards by supporting Federal Information Processing Standards (FIPS). For Change Guardian to run in FIPS mode, you must configure it after you install the Change Guardian server. For more information, see “Configure Change Guardian to Run in FIPS Mode” on page 35.

Traditional Change Guardian server Installation

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

You can install the Change Guardian server on your own Linux server, where you own both the hardware and the full Linux operating system that is installed on your hardware. If you want to install the managed software appliance, see “Appliance Change Guardian server Installation” on page 31.

RPM Prerequisites

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

- bash
- bc

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

NOTE: For SLES11SP4 platform, enable SLES11-Security-Module to install the curl-openssl1 package before installing Change Guardian 5.0 or higher versions.

To install the Change Guardian server interactively:

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

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

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

   `./install-changeguardian.sh`

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

   ---

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

   If you select standard, installation proceeds with the 60-day evaluation license key included with the installer. This license key activates the full set of product features for a 60-day evaluation period. At any time you can replace the evaluation license with a license key you have purchased.
5. (Conditional) If you select the custom configuration, complete the configuration using the following information:

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

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

Assign dbauser account password: PostgreSQL database maintenance account.

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

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

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

Configure FIPS mode: Configuring FIPS using the custom configuration is not currently supported. For more information about configuring Change Guardian to run in FIPS mode, see "Configure Change Guardian to Run in FIPS Mode" on page 35.

6 Create an admin account password for global system administration.

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

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

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

---

9 Configure the default email host using the following information:

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

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

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

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

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

Appliance Change Guardian server Installation

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

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

The Change Guardian appliance image is packaged in both ISO and OVF formats that can be deployed to the following virtual environments. For information about supported virtualization platforms, see the Technical Information page.

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

To install the Change Guardian server appliance image:

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

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

     ```
     tar -zxvf change_guardian_server_x.x.x.x.x86_64-0.xxxx.0.ovf.tar.gz
     ```
   - **2b** For VMWare, log in to the vSphere client and deploy the OVF template. For more information, see the VMWare documentation.
   - **2c** For Xen, launch XenCenter and import the OVF template. For more information, see the Xen documentation.

     NOTE: Do not select **Verify OVF manifest**. Do select **Use operating system fixup**.
3. (Conditional) If you are using Microsoft Hyper-V (Hyper-V documentation) or installing direct to hardware, use the ISO image to complete the following steps:
   - **3a** Burn the ISO file to a DVD or mount the image.

     NOTE: We do not support mounting the ISO image from a network share.
   - **3b** Start or reboot your computer and check the BIOS configuration of your machine. Your BIOS should allow you to start from the CD/DVD drive and change the order of the media.
   - **3c** (Conditional) If you have not mounted the image, boot the DVD.
4. Power on the appliance server.
5. Select the language and keyboard layout.
6. Read and accept the Novell SUSE End User License Agreement.
7. Read and accept the Change Guardian End User License Agreement.
8. Specify the hostname and domain name on the Hostname and Domain Name page, and verify that the **Assign Hostname to Loopback IP** option is selected.

   NOTE: Only select **Change Hostname via DHCP** if you do not have a static IP address reservation.
9. Set the Hardware Clock to UTC, specify the time zone of the VM, and select **Change** to configure NTP date/time synchronization.

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

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

10 Configure the following accounts:

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

11 Configure the default email host using the following information:

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

Configuring Change Guardian server

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

If you want Change Guardian to run in FIPS mode, you must complete additional steps. For more information, see “Configure Change Guardian to Run in FIPS Mode” on page 35.

Verify the Server Host Name

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

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

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

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

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

---

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

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

Ensure the Appropriate Server Ports Are Open

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

For SLES, use:

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

For RHEL, use:

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

For more information, see “Understanding Change Guardian Components” on page 12.

Configure the Server Date and Time Synchronization

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

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

Configure Server Certificates

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

1. su to `novell`.
2. cd to `/opt/novell/sentinel/setup`.
3. Generate certificate signing requests using the `./ssl_certs_cg` command, and make the following selections:
   - **3a** Generate certificate signing requests.
   - **3b** Web Server.
   - **3c** Specify a certificate signing request (`.csr`) filename.
   - **3d** Have your generated `.csr` file signed by a certificate authority.
4. Copy your CA root certificate chain (`ca.crt`) and the signed certificate (`.crt`) to `/opt/novell/sentinel/setup`.
5. Import the CA root certificate chain and the web server certificate with the following commands:
   - **5a** `./ssl_certs_cg`
   - **5b** At the menu prompt, select **Import certificate authority root certificate**.
   - **5c** Enter the CA root certificate chain file name (`ca.crt`).
   - **5d** At the menu prompt, select **Import certificate signed by certificate authority**.
   - **5e** When prompted, select **Web Server**.
   - **5f** Specify the name of the file that contains the CA’s signed digital certificate.
   - **5g** Select another service if necessary, or select **Done** and exit from the service option.
6. At the menu prompt, select **Exit** to exit from the TLS/SSL certificate configuration.

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

8 Import the CA root certificate change to the computer where you use the Change Guardian web console.

Change Default Email Host Settings

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

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

Verify the SHMMAX Setting

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

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

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

Configure Change Guardian to Run in FIPS Mode

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

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

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

2 (Conditional) If you want to change the keystore password, from a command prompt on the Change Guardian server, change directory to `/opt/novell/sentinel/bin` and enter the following script:

```
chg_keystore_pass.sh
```

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

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

```
./convert_to_fips.sh
```

4 Provide the requested input:

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

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

4c (Conditional) Provide the password for the `Web Server` keystore (the password you created in Step 2 on page 35)

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

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

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

```
Date_Timestamp|INFO|JAVOS listener|com.netiq.cg.capi.dao.UpgradeDao.upgrade
Upgrading EventDestination.Upgrade to fips compatible
Date_Timestamp|INFO|JAVOS listener|com.netiq.cg.capi.dao.UpgradeDao.upgrade
records updated=1 data={"service-host":"Server_Name","password":"Encrypted_Password","protocol":"vosrestdispatcher:rest
```

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

```
./convert_to_fips.sh
```

7 Provide the password for the FIPS keystore database (the password you created in Step 4b on page 35).

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

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

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

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

```
./convert_to_fips.sh
```

11 Provide the requested input:

11a Create the password for the FIPS keystore database.

11b Re-enter the password specified in Step 11a on page 36.

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

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

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

Configuring the Change Guardian Appliance for Updates

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

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

Register the Appliance with Customer Center for Updates

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

To register the appliance:

1. Obtain your appliance registration code or the appliance activation key.
2. Log in to the Change Guardian web console.
3. Click the **Registration** link.
4. Specify the following information:
   - Email ID to receive updates
   - System name
   - Appliance registration code

Configure Appliance Updates

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

- Subscription Management Tool (SMT) for secure environments where the appliance must run without direct Internet access
- Zypper for interactive updates

Configure Subscription Management Tool

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

1. Log in to the appliance console as the root user.
2. Refresh the repository for upgrade with the following command: `zypper ref -s`
3. Check whether the appliance is enabled for upgrade with the following command: `zypper lr`
4. Check the available updates for the appliance with the following command: `zypper lu`
5. Check the packages that include the available updates for the appliance with the following command: `zypper lp -r SMT-http_`*`smt_server_fqdn`*`:`*`package_name`*
6. Update the appliance with the following command: `zypper up -t patch -r SMT-http_`*`smt_server_fqdn`*`:`*`package_name`*
7. Restart the appliance.<Tanvi, to include SMT info from Sentinel docs>

For more information, see Configuring the Appliance with SMT in the *Sentinel Installation and Configuration Guide*.

5 Installing the Change Guardian Components

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

IMPORTANT: The installation process supports installing the Change Guardian Components in an administrator role.

Installing the Policy Editor

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

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

To install the Policy Editor:

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

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

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

Accessing the Policy Editor

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

Installing Windows Agents

You can install Windows agents in the following ways:

- Remotely install agents using the Agent Manager. For more information, see “Remote Installation” on page 40.
- Manually install the agent on a local computer. For more information, see “Manual Installation” on page 41.

NOTE: Agent Manager and the Windows agents will be in FIPS mode by default.

For information about requirements and recommendations for computers where you plan to install the agent, see the Technical Information page.

Remote Installation

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

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

To add assets to Agent Manager:

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

```
Hostname                    MajorType                   Addresses

houidam101.us.netiq.corp    Windows

houidam102.us.netiq.corp    Windows                     10.204.102.5
```

4b In the Agent Manager, click **Hosts List**.

4c Click **Browse**, navigate to the location where you saved the text file, and then click **Open**.

5 (Conditional) If you want to manually add an asset, do the following:

5a Click **Host**.

5b Specify the host name or IP address of the computer. To specify multiple IP addresses, use a comma to separate the addresses.

5c Select the appropriate operating system type, **Windows** or **Linux/UNIX** from the drop-down list.

5d Click **Add Assets**.

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

To install Windows Agent using Agent Manager:

1. From Change Guardian main, click **Integration** > **Agent Manager**.
2. Do one of the following:
   - (Conditional) If you have not previously added assets, in Agent Manager, under **Asset Groups**, click **All Assets** and then click **Add Assets**.
   - (Conditional) If you have previously added assets, in Agent Manager, click **All Assets**, then **Manage Assets**, and then **Add**.
3. From the assets list, select the computers where you want to deploy the agent. If you select multiple computers, they must all use the same credentials.
4. Log in as `root` to the computer that you want to connect and click **Next**.
5. Click **Manage Installation**, and then select **Install**.
6. Perform the following steps:
   1. For the agent version, select **Windows Agent *Agent Version***, where *Agent Version* is the version of the agent you want to deploy.
   2. For the agent configuration, you can choose the default configuration. If you want to modify the default configuration, use the **Edit** option to customize the default configuration.

      Otherwise, if required, you can add a new configuration using the **Add** option.
   3. Click **Start Installation**

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

NOTE: When you use the Agent Manager to install Windows agent, Agent Manager communicates with the agent via the Agent Management service.

Manual Installation

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

To manually install the Windows agents:

1. From Change Guardian main click, **Integration** > **Agent Manager**.
2. Click **All Assets**, and then click **Manage Installation** and select **Download**.

3 Download the agent artifacts and certificates. See “Downloading Agent Artifacts and Certificates” on page 42 section for the procedure.

4 Select the package you want to download and the configuration you want to use, and then click **Start Download**.

Agent Manager downloads `ChangeGuardianAgentforWindows.zip` to your computer.

5 Copy `ChangeGuardianAgentforWindows.zip` to the computer where you want to install the Windows agent and extract the files.

The silent installation package includes `NetIQCGAgentSilentInstaller.exe` and `NetIQCGAgentSilentInstaller.config`. Both files must be in the same directory. The configuration file contains the configuration you chose when you downloaded the silent installation package.

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

Downloading Agent Artifacts and Certificates

You must download the agent artifacts and its respective certificates package which contains the files that are necessary to install agents seamlessly.

When you download the agent artifacts and respective certificates, it is applicable for all the product agents. By default, during upgrade the existing agents will use the default certificates namely profile_iqc certificates. If you want to get newer certificates to ensure PCI compliance, you must switch the secure communication profile from profile_iqc to profile_javos. For more information, see “Secure Communication Profile” on page 26.

By default, during new installation of Change Guardian 5.0, the agents will use profile_javos certificates. If you have only Sentinel and/or Secure Configuration Manager installed, your agents will use the profile_iqc certificates by default.

NOTE: This is applicable for local installation and upgrade of Windows agents and Security Agent for UNIX.

To download the Agent certificates and artifacts:

1 In a web browser, access the Change Guardian web console at `https://server:8443`, where *server* is the IP address of the Change Guardian server.

2 When prompted, provide your Change Guardian user name and password.

3 Click **Integration** > **Agent Manager**.

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

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

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

7 Copy and extract `ChangeGuardianAgentCertificates.zip` file to the offline installer directory, before installing the agents.

Installing Security Agent for UNIX

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

Managing Change Guardian Modules

The Change Guardian Module Manager provides you with information about licensed modules, allows you to import module licenses to the Policy Editor, and allows you to remove module licenses from the Policy Editor.

To use the Module Manager, start the Policy Editor, click **Change Guardian**, and then select **Module Manager** in the navigation pane.The right pane displays the **Installed Modules**. By default, all the modules are selected. You can use the **Install** > **From Local Directory** option to install the modules.

The Licenses area displays the licenses of the modules that are applied, expiration date and the status. When you install Change Guardian, all available modules are installed automatically. Then you must import the license key for each module you want to use. To import license keys, click **Import License Key**, and then select the license key for the modules you want to use. After you import the license keys, you can use the module to create and assign policies.

6 Setting Up Your Environment for Monitoring

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

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

Understanding Policies

Policies allow you to define how Change Guardian monitors assets in your environment. A policy includes one or more constraints to define a specific change event you want to monitor in your enterprise.

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

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

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

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

Creating Policies

You can create a policy in the following ways:

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

Creating a Policy

To create a policy:

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

NOTE: For more information about enabling a policy, see “Enabling a Policy Revision” on page 48.

Cloning a Template

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

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

1. In the left pane of Policy Editor, select one of the following:
   - Active Directory
   - Group Policy
   - UNIX
   - Windows
   - Azure Active Directory
2. Expand the list of templates and select the template you want to clone. For example, **Active Directory Templates > AD Object > Site Link Cost Modified**.
3. Click **Apply**.
4. On the policy details window, make the appropriate changes, and then click **Submit**.
5. (Conditional) If you want to enable the policy now, select the **Enable this policy revision now** checkbox.

NOTE: For more information about enabling a policy, see “Enabling a Policy Revision” on page 48

Cloning a Policy

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

Understanding Event Severity

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

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

Understanding Managed Users

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

If you specify a user group as a managed user, as group membership changes, Change Guardian synchronizes policies with the new group members. For more information, see “Understanding LDAP Settings” on page 51.

Understanding Event Context

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

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

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

Enabling a Policy Revision

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

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

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

If you modify and enable a policy revision already assigned to computers, Change Guardian updates that policy to all computers with the policy assigned. When you update the enabled revision of a policy, Change Guardian automatically updates any monitored assets that have that policy assigned with the new revision. The Change Guardian Server does not automatically send an update, it marks the policy as new or updated.The agent will not get the updated or new policy assignment until it requests to heartbeat again.

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

To enable a policy revision from a module window:

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

Exporting and Importing Policies

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

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

To export a policy:

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

To import a policy:

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

Understanding Policy Sets

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

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

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

To access the Policy Set Manager:

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

After you create a policy set, you can assign the set as you would assign a policy. For more information, see “Assigning Policies and Policy Sets” on page 52.

Understanding Event Destinations

An **event destination** is where Change Guardian sends incoming events for a particular policy. You can view information about access and changes to critical files, systems, and applications. It is also where you deploy alert rules to notify you of those changes. For more information about alerts, see Chapter 15, “Understanding Alerts,” on page 119.

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 SIEM.

You can create and assign additional event destinations to meet your environment and regulatory needs. You can also change the default event destination setting.

If you set another event destination as the default, all new policies automatically use the new default location. Existing policies will continue to use their previously assigned event destinations. To change the event destinations for existing policies, see “Assigning Event Destinations to Policies” on page 50.

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 “Ensuring Alternate Event Destinations Receive Alerts” on page 121.

For more information about the Sentinel, see Sentinel Documentation.

If the Change Guardian server is configured to send its events to Sentinel, you can view Change Guardian events in Sentinel. To verify whether Change Guardian is configured, contact your system administrator.

Sentinel is a Security Information and Event Management (SIEM) solution that receives information from many sources throughout an enterprise, standardizes it, prioritizes it, and presents it to you to make threat, risk, and policy decisions.

Creating an Event Destination

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

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

To create an event destination:

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

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

Assigning Event Destinations to Policies

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

To assign event destinations to a policy:

1. Log in to the Policy Editor.
2. Click **Policy Assignment**.
3. Select an asset group or computer, and click **Assign Policies**.
4. Select a policy set or policy and click **Advanced**.
5. Select one or more event destinations to assign to the specified policy or policy set.
6. Click **OK**.

Understanding LDAP Settings

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

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

To access and configure the domain controller in LDAP settings, perform the following steps:

1. Click **Settings > LDAP Settings**.
2. In the **LDAP Settings** window, click **New**.
3. Specify the following fields:
   - **Domain name**: Specify the name of the Active Directory domain. For example, `test.example.com`
   - **User name**: Specify the name of the Active Directory user name. You can specify the user name in the following format:
     - `<user_name>`
     - `<domain_name\user_name>`
     - `<user_name@domain_name.com>`
   - **Password**: Specify the password for the Active Directory user.
   - **Polling interval**: It is the time interval at which the Change Guardian server synchronizes with the active directory for delta information.
4. Click **Test** button, to test the authentication of the Active Directory user before searching for the LDAP object.
5. Click **Apply** to save the configuration.

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

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

Understanding and Managing Asset Groups

Asset groups allow you to perform the following tasks:

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

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

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

Change Guardian supports the following types of asset groups:

- **Default groups** match specific platforms. You can view the members of default groups, but you cannot modify or delete the groups.
- **Static groups** contain only the assets you manually add to them. To add or remove members, you must manually update the group.
- **Dynamic groups** contain all assets that match the filter criteria you specify for the group. You can modify the filter criteria, but you cannot add or remove specific assets manually. Every 30 minutes, Change Guardian refreshes the group membership according to the specified criteria.

- **Assets** displays a list of all computers with Change Guardian agents installed. On the **Attributes** tab, you can view the computer attributes, such as computer name and operating system, and the groups to which the computer belongs. If you have the appropriate permissions, you can use the **Membership** tab to modify the computer's membership in static asset groups.

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

Assigning Policies and Policy Sets

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

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

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

Understanding Monitoring Schedules

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

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

Examples of valid time restrictions include:

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

To create a monitoring schedule:

1. Log in to the Policy Editor.

2. Click **Settings > Schedule Monitoring Time**.
3. Click **Add**.
4. In the **Schedule Time** window, select the time(s) and day(s) you want Change Guardian to stop monitoring, and then select **Don't Monitor**.

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

5. Click **OK**.

Understanding Change Guardian Email Alerts

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

- Install an email server on each event destination computer in your Change Guardian environment.
- Use the Policy Editor to:
  - Add each email server to Change Guardian.
  - Create one or more notification groups for each email server.
- Use the Change Guardian web console to assign email alerts to specified events. For more information, see "Assigning Email Alerts to Events" on page 73.

Adding Email Servers to Change Guardian

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

Prerequisite: Complete the following steps before you add an email server to Change Guardian:

1 (Conditional) To add email server to Change Guardian is in FIPS mode:

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

1b Import the certificate using the following command: `convert_to_fips -i <certificate_path>`.

1c Restart the Change Guardian server using the following command: `rcsentinel restart`.

1d Add new email configuration with STARTTLS protocol using Policy Editor.

1e Create routing rules in Change Guardian web console.

2 (Conditional) To add email server to Change Guardian is in non-FIPS mode:

2a Export the certificate from the respective SMTP server site.

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

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

2c Restart the Change Guardian server using the following command: `rcsentinel restart`.

2d Add new email configuration with STARTTLS protocol using Policy Editor.

2e Create routing rules in Change Guardian web console.

To add an email server to Change Guardian:

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

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

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

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

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

Creating and Configuring Notification Groups

For each email server you add to Change Guardian, you must create one or more notification groups specific to that email server. A notification group specifies one or more recipients of the email alerts and contains change event information. When you assign email alerts to events in the Change Guardian web console, you can choose from the notification groups available for that email server. For more information, see “Assigning Email Alerts to Events” on page 73.

To create and configure a notification group:

1. In the Policy Editor, select **Settings > Email Configuration**.
2. Select the email server for which you want to create a notification group.
3. Under **Notification Groups**, click **Add**.
4. Specify the name and description of the notification group you want to create.
5. Specify values for the following fields:
   - **From.** The return email address appearing on each email alert for this email server.
   - **To.** A list of email addresses, separated by commas, that receive email alerts.
   - **CC.** A list of email addresses, separated by commas, that receive copies of email alerts.

- **BCC.** A list of email addresses, separated by commas, that receive blind copies of email alerts.
- **Subject.** The subject for the alert email.
- **Maximum Events per Email.** Specifies the maximum number of events in the email alert.
- **Include Change Details.** Specifies whether the body of the email contains the details of the change detected by Change Guardian.
- **Email Format.** Specifies either text or HTML.

Using Change Guardian Administrative Reports

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

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

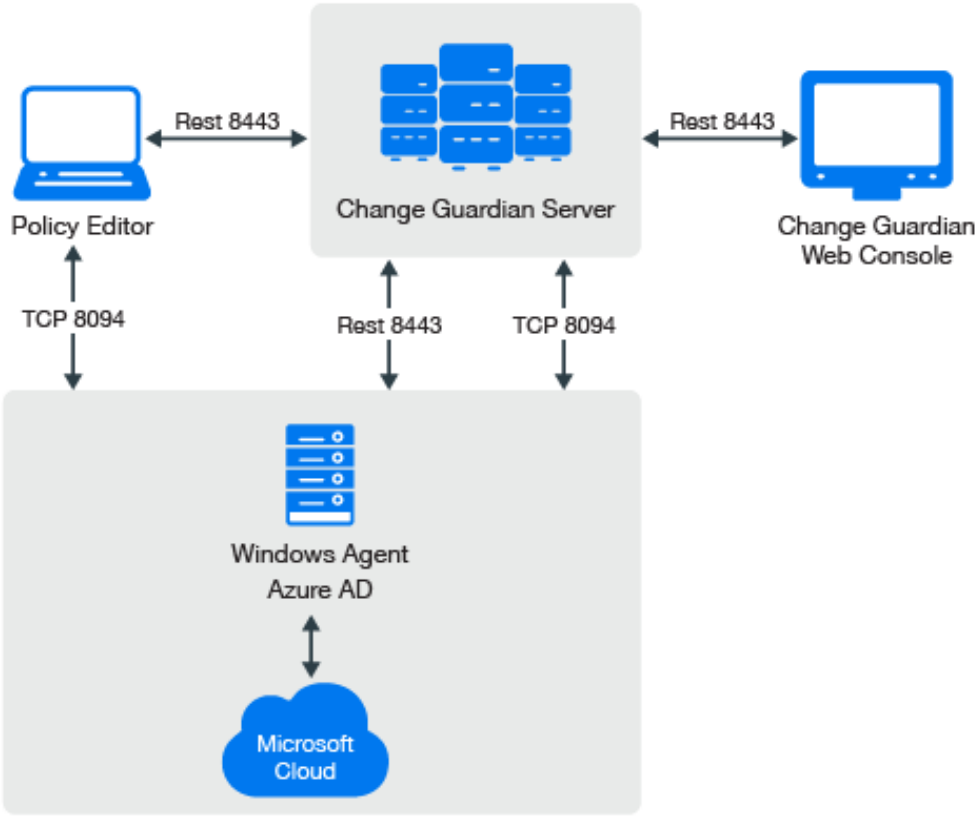
Understanding Azure Active Directory for Change Guardian

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

Change Guardian can monitor the following:

- Azure AD users
- Azure AD groups
- Azure AD roles for users and groups

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



Change Guardian connects with Azure Active Directory using the Microsoft Azure AD Reporting API. It supports a single tenant.

NOTE: The Azure AD agent is supported on Windows platforms. Change Guardian supports the user and group event types.

Planning Azure AD Monitoring Using Change Guardian

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

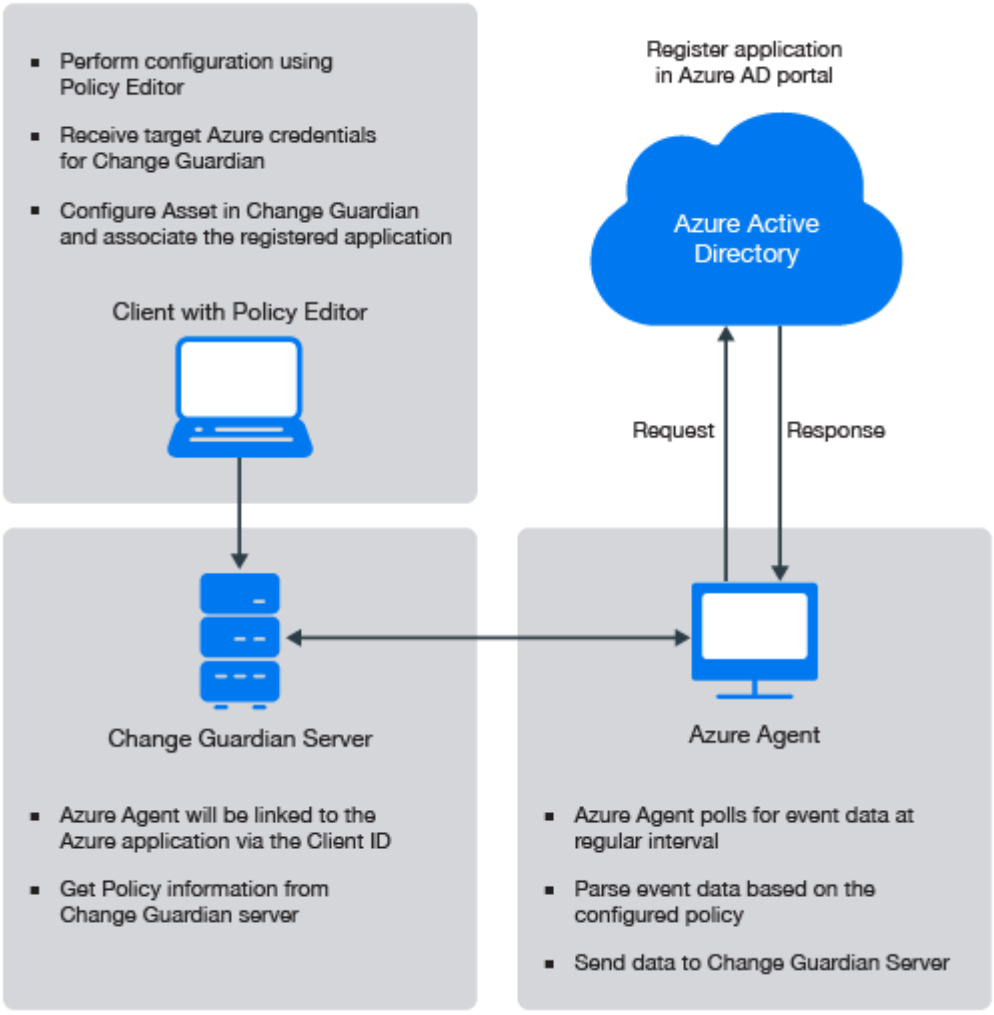
Task	See...
Ensure that you have created a tenant and its credentials are available for Change Guardian. Required credential details: ◆ Domain Name ◆ Client secret key ◆ Client ID	Microsoft Azure AD portal
Assign the license key for Azure AD module manually.	“Adding a License Key” on page 20
Create the Azure AD web application.	Microsoft Azure AD portal
Configure the Microsoft Azure tenant.	“Configuring Azure AD Tenant” on page 58
Create policies for users and groups.	“Creating a Policy for Azure AD Groups” on page 59 “Creating a Policy For Azure AD User Accounts” on page 59
Assign policies and view events on the Change Guardian web console.	“Assigning a Policy to an Asset” on page 59
(Conditional) Configure the default Windows registry keys, if you want to modify the default keys based on your requirements.	“Configuring Default Windows Registry Keys” on page 60
(Conditional) During upgrade, ensure that you reconfigure the Windows agent to enable Azure AD monitoring.	“Reconfigure Windows Agent to Monitor Azure AD Using Agent Manager” on page 61
Triage events.	You can triage events in the Change Guardian web console and click the Change Guardian shield to get more information about the events.

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

Change Guardian supports real-time monitoring. But, due to latency limitation from Microsoft Azure, Change Guardian is experiencing delay in fetching audit logs. This limitation can be overcome when Microsoft fixes this latency issue.

IMPORTANT: Change Guardian supports monitoring on the Microsoft Azure public cloud. For more information, see Azure FAQs.

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



Configuring Azure AD Tenant

In Azure Active Directory (Azure AD), a tenant is a representative of an organization. You have to configure a tenant and its credentials such as Domain Name, Client secret key, and Client ID and make it available for Change Guardian.

Complete the following steps to configure the Azure AD tenant for monitoring, using the Policy Editor:

1. Select **Azure Active Directory** from the left panel of the Azure AD portal.
2. From the tree, navigate to **Azure Tenant Configuration**.
3. In the **Azure Tenant Configuration** window, specify values for the following fields:
   - **Domain Name**: Specify the name of the Azure Active Directory domain.
   - **Client ID**: Enter the Client ID that was displayed in the Azure portal during configuration.
   - **Client Secret Key**: Enter the Client secret key that was displayed in the Azure portal during configuration.
   - **Comment**: (Optional) Enter a comment.

4. Click **Save**.
5. (Conditional) If you want to modify any particular configuration, you need to make the modifications in the **Azure Tenant Configuration** window.

Creating a Policy for Azure AD Groups

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

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

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

4. Click **Submit**.

Creating a Policy For Azure AD User Accounts

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

1. In the left pane of the Policy Editor window, select **Azure Active Directory** > **Azure Active directory Policies**.
2. Expand the **Azure Active directory Policies** and select **User Accounts**.
3. Click **Create Policy**.
4. On the **User Account Policy** window, specify the appropriate information.

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

5. Click **Submit**.

Assigning a Policy to an Asset

Complete the following steps to assign a policy:

1. In the left pane of the Policy Editor window, navigate to **Change Guardian**.
2. Click **Policy Assignment**.
3. Select an Azure asset group or computer, and click **Assign Policies**.
4. Select **Assets** from the drop-down list.

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

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

Configuring Default Windows Registry Keys

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

- “Configuring Azure AD Event Fetching Interval” on page 60
- “Configuring Azure AD Access Token Refresh Time Interval” on page 60
- “Configuring Azure AD Event Collection Interval” on page 61

Configuring Azure AD Event Fetching Interval

By default, Change Guardian sets the time interval to 120 minutes behind the *current system time* as the *start time* to fetch the events due to latency issues from Microsoft Azure AD Reporting API. Change Guardian does deduplication of events internally to avoid any duplicate events while processing the events once Change Guardian receives the events from Azure AD. For more information, see Azure Active Directory reporting latencies.

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

1. In Windows registry settings, navigate to the Change Guardian Agent installation directory:

   `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\NetIQ\ChangeGuardianAgent`
2. Right click the `AzureADEventFetchInterval` key.
3. Select **Decimal** under **Base**.
4. (Conditional) If you notice a higher latency value in your environment, you can configure this value based on your observed value. The value range is between 120 minutes to 1440 minutes (24 hours) for the **Value data** field.

   NOTE: If you configure this value to above 1440 minutes, it will reset it to 1440 minutes by default, since that is the maximum value. If the latency from Microsoft is more than this value, you might face a data loss.

   ---
5. Click **OK**.
6. Go to **Services** > **Change Guardian Agent**.
7. Select the Change Guardian Windows Agent application, then click **Restart**.

Configuring Azure AD Access Token Refresh Time Interval

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

If you want to modify this time interval based on your requirement, complete the following steps:

1. In Windows registry settings, navigate to the Change Guardian Agent installation directory:

   `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\NetIQ\ChangeGuardianAgent`
2. Right click the `AzureADTokenRefreshInterval` key.
3. Select **Decimal** under **Base**.

4. Specify the time interval to any required value range between 15 minutes to 50 minutes in the **Value data** field.
5. Click **OK**.
6. Go to **Services** > **Change Guardian Agent**.
7. Select the Change Guardian Windows Agent application, then click **Restart**.

Configuring Azure AD Event Collection Interval

By default, Change Guardian fetches the events every 10 minutes from Azure Active Directory. The recommended periodicity value is10 minutes.

The default minimum value is 5 minutes and the maximum value is 30 minutes. If you configure this value to below 5 minutes, the system will reset it to 5 minutes automatically. If you configure this value to above 30 minutes, the system will reset it to 30 minutes automatically.

If you want to modify this time interval based on your requirement, complete the following steps:

1. In Windows registry settings, navigate to the Change Guardian Agent installation directory:

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

Reconfigure Windows Agent to Monitor Azure AD Using Agent Manager

During new installation of Change Guardian 5.0 or upgrade from Change Guardian 4.2 or later to Change Guardian 5.0 if you want to monitor Azure AD, you must deploy Windows agent 5.0 version and enable Azure AD monitoring using the Change Guardian Agent Manager.

Perform the following steps to deploy and reconfigure Windows agent to enable Azure AD monitoring:

1 From Change Guardian main, click **Integration** > **Agent Manager**.

2 Do one of the following:

- (Conditional) If you have not previously added assets, in Agent Manager, under **Asset Groups**, click **All Assets** and then click **Add Assets**.
- (Conditional) If you previously added assets, in Agent Manager, click **All Assets** > **Manage Assets**, and then click **Add**.

3 From the assets list, select the computer where you want to deploy an agent. You can select multiple computers if Agent Manager can use the same credentials to connect to the computers.

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

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

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

6 Perform the following steps:

1. For the agent version, select **Change Guardian Agent for Windows *Agent Version***, where *Agent Version* is the version of the Windows agent you want to deploy.
2. For the agent configuration, click add a new configuration using the **Add** option. Fill in all the details.
3. For **Enable Azure AD Monitoring** option, select **Yes** to specify that you want to reconfigure the Windows agent to enable Azure AD monitoring.
4. Click **Start Reconfiguration**.

Troubleshooting

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

Receiving an Invalid Token

Issue: Change Guardian is unable to receive events because of the Incorrect Domain Name, Client secret key, or Client ID.

Workaround: Obtain the correct Domain Name, Client secret key, or Client ID from the Microsoft Azure AD portal.

NOTE: Severity of the *Invalid token* event varies based on the severity of the first policy that was assigned. If the policy assigned is of the *automatic* severity, the severity of *Invalid token* event will be set to 4.

Change Guardian Is Unable to Receive Azure AD Events

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

- Incorrect Domain Name, Client secret key or Client ID.
- Tenant is not reachable
- Invalid remote web application

Workaround:

- Obtain the correct Domain Name, Client secret key or Client ID from the Microsoft Azure AD portal.
- Enter a valid tenant name in the tenant configuration page.
- Check if the tenant is accessible from the Change Guardian Agent computer.

Configuring Your Active Directory Environment

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

- Security event log

- Active Directory auditing
- Active Directory security access control lists (SACLs)

NOTE: You must restart the Active Directory tools, whenever you restart the Windows Agent.

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

Configuring the Security Event Log

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

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

To configure the security event log:

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

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

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

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

Configuring Active Directory Auditing

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

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

To verify or set this configuration:

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

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

   ---

5. Expand **Computer configuration > Policies > Windows Settings > Security Settings**.
6. Complete the following steps:
   - **6a** In **Security Settings**, expand **Advanced Audit Policy Configuration > Audit Policies**.
   - **6b** For CGAD and CGGP, click **DS Access**.
   - **6c** For each subcategory, configure or verify the following selections:
     - Configure the following audit events
     - Success
     - Failure
   - **6d** For CGAD only, define the same configuration for all subcategories of **Account Management** and **Policy Change**.
7. Complete the following steps:
   - **7a** In **Security Settings**, expand **Local Policies** and click **Audit Policy**.
   - **7b** For CGAD and CGGP, click **Audit directory service access**.
   - **7c** Configure or verify the following selections:
     - Define these policy settings
     - Success
     - Failure
   - **7d** For CGAD only, configure or verify the same selections for **Audit account management** and **Audit policy change**.
8. Return to the command prompt, type `gpUpdate` and press **Enter**.

Configuring User and Group Auditing

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

You can configure user and group auditing manually.

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

To manually configure user and group auditing:

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

Configuring Active Directory Security Access Control Lists

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

To monitor all changes of current and future objects inside Active Directory with Change Guardian for Active Directory, follow the steps in “Configuring SACLs for Change Guardian for Active Directory” on page 66. If you are running only Change Guardian for Group Policy in your environment, see “Configuring SACLs for Change Guardian for Group Policy Only” on page 67.

Configuring SACLs for Change Guardian for Active Directory

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

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

To verify or set this configuration:

1. Log in to a computer in the domain you want to configure using a user account with domain administrator privileges.
2. Open a command prompt, type `adsiedit.msc` and press **Enter** to start the ADSI Edit configuration tool.
3. Right-click **ADSI Edit**, and then select **Connect to**.
4. In the Connection window, ensure that **Name** is set to `Default naming context`, and **Path** points to the domain to configure.

   NOTE: You must perform Step 5 through Step 13 three times, configuring the connection points for **Default naming context**, **Schema**, and **Configuration**.

   ---

5. In **Connection Point**, select **Select a well known Naming Context**, and then select one of the following:
   - On the first time through this step, select **Default naming context** in the drop-down list.
   - On the second time through this step, select **Schema**.
   - On the third time through this step, select **Configuration**.
6. Click **OK**, and then expand **Default naming context** or **Schema** or **Configuration**.
7. Right-click the node under the connection point (begins with `DC=` or `CN=`), and select **Properties**.
8. On the Security tab, click **Advanced**.
9. On the Auditing tab, click **Add**.
10. Configure auditing to monitor every user.
    - ***If you are using Windows Server 2012:***
      1. Click **Select a principal**.
      2. Type `everyone` in the **Enter the object name to select** field.
      3. Click **OK**.
      4. In the **Type** field, select **All**.
      5. In the Permissions list, select the following:
         - Write All Properties
         - Delete
         - Modify Permissions
         - Modify Owner
         - Create All Child Objects

         The other nodes related to child objects are selected automatically.

- Delete All Child Objects

  The other nodes related to child objects are selected automatically.

- ***For all other versions of Windows:***

  1. Type `everyone` in the **Enter the object name to select** field.
  2. Click **OK**.
  3. In the Access list, select **Successful** and **Failed** for the following:
     - Write All Properties
     - Delete
     - Modify Permissions
     - Modify Owner
     - Create All Child Objects

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

       The other nodes related to child objects are selected automatically.

11. In the **Applies to** or **Apply onto** field, select **This object and all descendant objects**.
12. Clear the setting to **Apply these auditing entries to objects and/or containers within this container only**.
13. Click **OK** until you close all open windows.
14. Repeat Step 5 through Step 13 two more times.

Configuring SACLs for Change Guardian for Group Policy Only

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

To verify or set this configuration:

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

---

1. Log in to a computer in the domain you want to configure using a user account with domain administrator privileges.
2. Open a command prompt, type `adsiedit.msc` and press **Enter** to start the ADSI Edit configuration tool.
3. Right-click **ADSI Edit**, and then select **Connect to**.
4. In the Connection window, ensure **Name** is set to `Default naming context`, and **Path** points to the domain to configure.
5. In **Connection Point**, select **Select a well known Naming Context**, and then select **Default naming context** in the drop-down box.
6. Click **OK**, and then expand **Default naming context**.
7. Right-click the node under the connection point (begins with `DC=`), and select **Properties**.
8. Select the **Security** tab.
9. Click **Advanced** > **Auditing** > **Add**.

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

5. In the **Permissions** list, select the following:
    - Delete
    - Create Sites Container objects
6. In the **Properties** list, select the following:
    - Write gPLink
    - Write gPOptions

- ***For all other versions of Windows:***
    1. Type `everyone` in the **Enter the object name to select** field.
    2. Click **OK**.
    3. In the **Permissions** list, select the following:
        - Delete
        - Create Sites Container objects
    4. In the **Properties** list, select the following:
        - Write gPLink
        - Write gPOptions

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

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

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

Synchronizing Active Directory User Accounts

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

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

To view and manage synchronized Active Directory accounts:

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

2 Click **AD Accounts**.

Adding a User Container

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

To add a user container to Change Guardian:

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

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

Mapping User Profile Fields

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

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

7 Viewing Change Guardian Events

This chapter describes using the Change Guardian web console to view **events**, which are the results from assigned policies and policy sets, in event reports. To access the web console, specify the following web address, as determined by your Change Guardian sever installation:

`https://Change_Guardian_Server_IP_Address:8443`

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

Supported Web Browsers and Settings

You can view Change Guardian event reports from a Windows or Linux computer with one of the web browsers installed. For information about the recommended browsers, see the Change Guardian Technical Information website.

Understanding Event Information

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

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

NOTE: Events related to binary files include only delta information.

Viewing Detailed Event Information

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

To see detailed event information, click the shield icon.

People

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

To view the user identity details of an event:

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

If you do not have Identity Manager or a similar product installed, this option is not available. For more information about integrating identity information with Change Guardian events, see “Integrating Identity Information” in the *Sentinel Administration Guide*.<Tanvi to include this info from Sentinel guide>

Tags

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

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

Filters

Filters allow you to customize event searches and prevent data overload. The Filter Builder helps you build search queries ranging from simple to complex. You can save a search query as a filter and reuse it at any time to quickly perform a search instead of manually building the query again.

For more information about filters, see Chapter 13, “Configuring Filters,” on page 107.

Assigning Email Alerts to Events

To send email messages from within the Change Guardian web console, you must create an event routing rule, and you must have an email server configured for the web console computer. If you do not have an email server configured, no notification groups appear as available actions for the event routing rule. For more information about configuring email servers, see “Understanding Change Guardian Email Alerts” on page 53.

To assign email alerts to an event:

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

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

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* <Tanvi to include this info from Sentinel guide>.

8 Configuring Event Routing Rules

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 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.

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.

Creating an Event Routing Rule

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.

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

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

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

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

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

   - **All:** Routes the event to all services including Correlation, Security Intelligence, and Anomaly Detection.
   - **Event store only:** Routes the event to the event store only.
   - **None (drop):** Drops or ignores the events.

   Perform the following actions: Select an action to be performed on every event that meets the filter criteria.

   Select the email configuration that you already created using Policy Editor. For more information see, “Adding Email Servers to Change Guardian” on page 53 and “Creating and Configuring Notification Groups” on page 54

   The actions listed here are different than the actions displayed in the **Event Actions** tab in the Change Guardian Main interface, and are distinguished by the `<EventRouting>` attribute in the `package.xml` file created by the developer.
3. Click **Save** to save the event routing rule.

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

Ordering Event Routing Rules

When there is more than one event routing rule, the event routing rules can be reordered by dragging them to a new 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.

1. From Change Guardian main, click **Routing** in the toolbar.

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

   Existing event routing rules appear on the page.
2. Mouse over the icon to the left of the event routing rule numbering to enable drag-and-drop. The cursor changes.
3. Drag the event routing rule to the correct place in the ordered list.

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

Activating or Deactivating an Event Routing Rule

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

1. From Change Guardian main, click **Routing** in the toolbar.

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

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

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

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

9 Configuring Roles and Users

In Change Guardian, you can add, edit, and delete roles. You can also grant different permissions at the role level, and edit the details of user and role profiles.

Overview

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

Change Guardian has the following roles by default:

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

You cannot modify or delete the administrator role.

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

Operator A user in this role can manage alerts, view Security Intelligence Dashboards, share alert and event views, run reports, view and rename reports, and delete report results. The Threat Response dashboard allows Operators to triage alerts quickly and efficiently.

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

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

Creating Roles

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

Creating a Role

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

Users created under this role will have access to view events from the selected tenant.

3 Click **Create** in the **Roles** section to create a new role.

4 Use the following information to create the role:

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

Description: Specify a description of the role.

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

- **View all event data:** Select this option to allow users to view all the data in the Change Guardian system. If you select this option, you must select one or more of the following permissions:
- **View the following data:** Select this option to allow users to view only selected data in the Change Guardian system.
  - **Only events matching the criteria:** Allows users to view only the events returned by the specified search query. For example, if you set the filter value to `sev:5`, users with this permission can view only events of severity five in a search.
  - **Search Data Targets:** When this permission is set on a role, all members of that role can perform searches on Change Guardian systems that are in a distributed location.
  - **View asset data:** Allows users to view asset data.
  - **View asset vulnerability data:** Allows users to view vulnerability data.
  - **View data in the embedded database:** Allows users to view the data in the embedded database.
  - **View people browser:** Allows users to view the data in the Identity Browser.
  - **View system events:** Allows users to view the Change Guardian system events.
- **Allow users to access reports:** Select this option to allow users to access and manage reports.
  - **Manage reports:** Allows users to create, modify, run, and delete reports.
  - **Run reports:** Allows users to only run reports.
- **Allow users to manage alerts:** Select this option to allow users to view and manage alerts. Select either of the following options:
  - **Manage all alerts:** Allows the users to view and edit all the alerts and configure alert creation.
  - **Manage only alerts that match the following criteria:** Allows the users to view and edit the alerts that match the specified criteria. This permission also allows the role to configure alert creation.
- **Sharing:** Allows users in the role to share real-time views, filters, and reports with other users.
- **Miscellaneous:** Assign miscellaneous permissions as necessary:
  - **Edit knowledge base:** Allows users to view and edit the knowledge base in the **Alert Details** page.
  - **Manage Tags:** When this permission is set on a role, all members of this role can create, delete, and modify tags, and associate tags to different event sources.
  - **Manage roles and users**: Allows non-administrator users to administer specific roles and users.
  - **Proxy for Authorized Data Requestors**: When this permission is set on a role, the members of this role can accept searches from remote data sources.

- **View and execute event actions:** When this permission is set on a role, all members of this role can view events and execute actions on the selected events.
- **View detailed internal system state data:** When this permission is set on a role, all members of this role can view detailed internal system state data by using a JMX client.
- **View knowledge base:** Allows users to view the knowledge base in the **Alert Details** page.

5 Click **Save**.

To create users for this role, see "Creating Users" on page 80.

Configuring Password Complexity

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

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

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

The following table describes the password complexity validation rules:

Table 9-1 *Password Complexity Rules*

Validation Rule	Description
MINIMUM_PASSWORD_LENGTH	Specifies the minimum number of characters required in a password.
MAXIMUM_PASSWORD_LENGTH	Specifies the maximum number of characters allowed in a password.
UNIQUE_CHARACTER_LENGTH	Specifies the minimum number of unique characters required in a password. For example, if the UNIQUE_CHARACTER_LENGTH value is 6 and a user specifies the password as "aaaabbccc", the Change Guardian does not validate the password because it contains only 3 unique characters a, b, and c.
LOWER_CASE_CHARACTERS_COUNT	Specifies the minimum number of lowercase characters required in a password.
UPPER_CASE_CHARACTERS_COUNT	Specifies the minimum number of uppercase characters required in a password.
ALPHABET_CHARACTERS_COUNT	Specifies the minimum number of alphabetic characters required in a password.
NUMERIC_CHARACTERS_COUNT	Specifies the minimum number of numeric characters required in a password.

Validation Rule	Description
NON_ALPHA_NUMERIC_CHARACTERS_COUNT	Specifies the minimum number of non-alphanumeric or special characters required in a password. The rule considers only the following non-alphanumeric characters: ` ~ ! @ # $ % ^ & * ( ) - _ = + [{] } \ | ; : ' " < , > . / ?
RESTRICTED_WORDS_IN_PASSWORD	Specifies the words that are not allowed in a password. The restricted words are case-insensitive. You can specify multiple words separated by a comma. For example,RESTRICTED_WORDS_IN_PASSWORD= admin,password,test

Creating Users

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

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

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

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

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

   Directory: The **Directory** option is enabled only if you have configured the Change Guardian server for LDAP authentication. Select this option for the server to authenticate the user log in against an LDAP directory.
6. (Conditional) If you specified Local for the authentication type in Step 5, specify any user name in the Username field and continue with Step 8.
7. (Conditional) If you specified Directory for the authentication type in Step 5, specify the user name according to the settings you used when you configured LDAP, then continue with Step 10.
8. Specify a password in the **Password** field.

   NOTE: For local user password, ensure that the password adheres to the password complexity validation rules. For more information, see “Configuring Password Complexity” on page 79.
9. Re-enter the password in the **Verify** field.
10. The **Title**, **Office #**, **Ext, Mobile #**, **and Fax.** fields are optional. The phone number fields allow any format. Make sure you enter a valid phone number so that the user can be contacted directly.
11. Click **Save**.

10 Reporting

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.

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

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

This chapter provides information about the following:

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.

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 in the Change Guardian Main interface 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 Chapter 19, “Configuring Data Federation,” on page 143.

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 83.

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 `novell` user.
2. Change to the `/etc/opt/novell/sentinel/config` directory:`cd /etc/opt/novell/sentinel/config/`
3. Open the `obj-component.JasperReportingComponent.properties` file for editing:

   `vi obj-component.JasperReportingComponent.properties`
4. 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/write permissions on the specified directory.
5. 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 in the web console. 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.

11 Configuring Tags

Tags are user-defined values that can be used to logically group data collection objects such as event sources, event source servers, 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.

NOTE: Only users in the Manage Tags role can create and manage tags.

Overview

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.

When ESM objects such as event sources and event servers, all the events from those ESM objects are tagged with that value. The tag value is placed in a reserved variable, `rv145`. However, events generated before tagging the ESM objects are not tagged. Change Guardian does not perform retroactive tagging of data that is already stored because it is not an accepted practice to modify events that are already stored.

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.

The Tags Interface

The Tags interface lists the tags available in the system and allows you to manage the tags. You can perform text-refined searches to find the tags that you are looking for. The interface also provides options such as maintaining a list of favorite tags and searching tagged events.

As you mouse over a tag, you can see the icons available to manage the tag. The number next to each tag indicates the number of objects associated with the tag. For more information on creating new tags, see "Creating a Tag" on page 88.

The **Tag** icon is available in various parts of the Change Guardian interface, which allows you to quickly add tags to the desired data collection objects such as event sources, event source servers, report templates, and report results. When you click the **Tag** icon, the Tags dialog box is displayed that allows you to select tags and to create new tags.

Creating a Tag

1. Log in to the Change Guardian Main interface as a user in the Manage Tags role.

   `https://<IP_Address/DNS_Sentinel_server:8443>/sentinel/views/main.html`

   IP_Address/DNS_Change Guardian_server is the IP address or DNS name of the Change Guardian server and *8443* is the default port for the Change Guardian server.

2. 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.
3. Click **Create**.
4. 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.

5. 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.

6. Click **Save**.

Managing Tags

Sorting Tags

You can sort tags either based on their names or based on the number of objects associated with the tags.

1. Log in to the Change Guardian Main interface 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.

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.

1. Log in to the Change Guardian Main interface 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.

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.

1. Log in to the Change Guardian Main interface 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.

1. Log in to the Change Guardian Main interface 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

1. Log in to the Change Guardian Main interface 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

You can associate tags with event sources, event source servers, 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

1. Log in to the Change Guardian Main interface as a user in the administrator role.
2. Click **Routing** in the toolbar, then click **Create**.
3. Specify a name and filter criteria for the rule.
4. Click **Select tag**, then select the tags that you want to associate with the rule.
5. Click **Set**.

Associating Tags with Event Sources

1. Log in to the Change Guardian Main interface as a user in the administrator role.
2. Select **Collection > Event Sources.**
3. Select the event sources that you want to associate with the tag.
4. Select the **Configure**  icon, then select **Tags**.
5. Select the tags you want to associate, then click **Set**.

Associating Tags with Event Sources Servers

1. Log in to the Change Guardian Main interface as a user in the administrator role.
2. Select **Collection > Event Sources.**
3. From the **Event Source Servers** section, select one or more event source servers that you want to associate with the tag.
4. Select the **Configure**  icon, then select **Tags**.
5. Select the tags you want to associate, then 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.

1. Log in to the Change Guardian Main interface.
2. Select **Reports** in the navigation panel on the left.
3. Select the report result or the report definition that you want to associate with a tag.
4. Do one of the following:
   - Select **Tags** from the **more** drop-down list.
   - Click **Edit** at the bottom left pane.
5. Select one or more tags that you want to associate with selected reports.
6. Click **Set**.

Viewing Tagged Events

1. Log in to the Change Guardian Main interface.
2. 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**.

12 Searching Events

Change Guardian provides an option to perform a 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.

By default, the search results include all events generated by the Change Guardian system operations. These events are tagged with the `Sentinel` tag. If no query is specified and you click **Search** for the first time after the Change Guardian installation, the default search returns all events with severity 0 to 5. Otherwise, the Search feature reuses the last specified search query.

To search for a value in a specific field, use the ID of the event name, a colon, and the value. For example, to search for an authentication attempt to Change Guardian by user2, use the following text in the search field:

```
evt:LoginUser AND sun:user2
```

An advanced search can narrow the search for a value to a specific event field. The advanced search criteria are based on the event IDs for each event field and the search logic for the index. Advanced searches can include the product name, severity, source IP, and the event type. For example:

- `pn:NMAS AND sev:5`

  This searches for events with the product name NMAS and severity five.

- `sip:10.0.0.01 AND evt:"Set Password"`

  This searches for the initiator IP address 10.0.0.1 and a “Set Password” event.

Multiple advanced search criteria can be combined by using various operators. The advanced search criteria syntax is modeled on the search criteria for the Apache Lucene open source package. For more information on building search criteria, see Appendix A, “Search Query Syntax,” on page 165.

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.

Searching Events Indexed in Traditional Storage

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. For more information, see Chapter 19, “Configuring Data Federation,” on page 143.

This section provides information about the following topics:

- “Saving a Search Query” on page 98
- “Performing Event Operations” on page 102

Performing a Search

To perform a search:

1. Log in to the Change Guardian Main interface:

   `https://<IP_Address/DNS_Change Guardian_server:8443>/sentinel/views/main.html`

   Where *IP_Address/DNS_Change Guardian_server* is the IP address or the DNS name of the Change Guardian server and *8443* is the default port for the Change Guardian server.
2. In the **Reports and Searches** panel, click **New search**.
3. You can perform a search by using any of the following:
   - **Search criteria:** Specify the search criteria in the **Search** field.

     For information on creating search criteria, see Appendix A, “Search Query Syntax,” on page 165.
   - **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**, and then click **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.
4. (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.
5. (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 19, “Configuring Data Federation,” on page 143.
6. Click **Search**.

   The search results are displayed. For information on the search results, see “Viewing Search Results” on page 95.
7. (Optional) Modify the search criteria by clicking Edit Criteria.
8. (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.

9 Click **Search**.

10 (Conditional) To save the search query, see “Saving a Search Query” on page 98.

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.

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.

Group	Icon	Description
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.
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:

Icon	Type of Event
	Audit event
	Performance event
	Anomaly event
	Correlation event
	Unparsed event

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.

- “Summary View” on page 96
- “Detailed View” on page 96

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 Log in to the Change Guardian Main interface.

   `https://<IP_Address/DNS_Change Guardian_server:8443>/sentinel/views/main.html`

   IP_Address/DNS_Change Guardian_server is the IP address or the DNS name of the Change Guardian server and *8443* is the default port for the Change Guardian server.

2 In the **Reports and Searches** panel, click **New Search**.

3 Specify the search criteria, then click **Search**.

   For more information on how to run an event search, see “Searching Events Indexed in Traditional Storage” on page 93.

4 Click **fields** in the REFINE section.The Select Event Fields window is displayed.

5 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.

6 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.

7 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.

8 Repeat Step 4 through Step 7 to further refine the search.

9 (Optional) Click **clear** to clear the selected unique event field values from the **REFINE** panel and to return to the original search results.

10 (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 98
- "Saving a Search Query as a Filter" on page 99
- "Saving a Search Query as a Report Template" on page 99
- "Saving a Search Query as a Routing Rule" on page 101
- "Saving a Search Query as a Retention Policy" on page 102

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 "Searching Events Indexed in Traditional Storage" on page 93 and "Refining Search Results" on page 97.

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 "Searching Events Indexed in Traditional Storage" on page 93 and "Refining Search Results" on page 97.

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 "Searching Events Indexed in Traditional Storage" on page 93 and "Refining Search Results" on page 97.

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.
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 19, “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.

Parameter	Description
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.
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 in the Change Guardian Main interface. To view the reports, see "Working with Reports" on page 83.

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, see “Searching Events Indexed in Traditional Storage” on page 93 and “Refining Search Results” on page 97.

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 Indexed in Traditional Storage” on page 93 and “Refining Search Results” on page 97.
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 19, “Configuring Data Federation,” on page 143.

Performing Event Operations

You can use the events in the search results to perform various tasks as you view the search results.

- “Viewing Asset Data” on page 104
- “Viewing Vulnerabilities” on page 105

Executing Actions

Only users in the following roles can execute actions on events:

- Administrator
- 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, see “Searching Events Indexed in Traditional Storage” on page 93 and “Refining Search Results” on page 97.
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.

Exporting the Search Results to a File

1. Perform a search, and refine the search results as desired.

   For more information, see “Searching Events Indexed in Traditional Storage” on page 93 and “Refining Search Results” on page 97.
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**.

Viewing Identity Details of Events

If Change Guardian is integrated with Identity Management systems, you can view the user identity details of events. You must have the View People Browser permission to view the Identity details.

1. Perform a search, and refine the search results as desired.

   For more information, see “Searching Events Indexed in Traditional Storage” on page 93 and “Refining Search Results” on page 97.
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.

Viewing Advisor Report

The following are the prerequisites to view the Advisor data:

- The Advisor feed must be up-to-date, processed, and loaded into the Change Guardian database.
- The selected event must be from a product supported by Advisor and it must have the Vulnerability field value set to 1.

To view the Advisor data:

1. Click **Filters** > **Exploit Detected Events** or specify vul:1 in the **Search** field, then click **Search**.

   All events that are likely to have exploited a known vulnerability are displayed.
2. In the search results, select the events for which you want to view the Advisor data.
3. Click **Event operations** > **View Advisor report**.

   The Advisor report is displayed in a new tab.

Viewing Asset Data

You must have the View Asset Data permission to view the asset data of the selected events. You can view the asset information related to a machine or device from which you are receiving events. To view the asset data, you must run the asset management Collector and ensure that the asset data is being added to the Change Guardian database.

1. Perform a search, and refine the search results as desired.

   For more information, see “Searching Events Indexed in Traditional Storage” on page 93 and “Refining Search Results” on page 97.
2. In the search results, select the events for which you want to view the asset data.
3. Click **Event operations** > **View assets**.

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.

   For more information, see “Searching Events Indexed in Traditional Storage” on page 93 and “Refining Search Results” on page 97.
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.**

13 Configuring Filters

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 you can perform a search by selecting the filter rather than specifying the query manually every time.

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** in 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.

To view events based on filters, select the desired filter. The associated events are displayed in the search results panel.

- "Creating Filters" on page 107
- "Sample Filters" on page 111
- "Viewing Events by Using Filters" on page 113
- "Managing Filters" on page 113

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 nothing but 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** link on the top right of the Change Guardian Main interface for a list of event field names and their IDs.

For information about the syntax for the criteria, see Appendix A, “Search Query Syntax,” on page 165.

- “Building a New Criteria” on page 108
- “Selecting an Existing Criteria” on page 109
- “Creating a Filter” on page 110

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.

For information about the syntax for criteria, see Appendix A, “Search Query Syntax,” on page 165.

The Build Criteria dialog box includes the following elements:

Table 13-1 *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. For information on creating a filter criteria (search query), see Appendix A, “Search Query Syntax,” on page 165. 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** located at the top right of the Change Guardian Main interface.

Element	Description
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.
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** located at the top right of the Change Guardian Main interface. ◆ 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" on page 110
- "Creating a Filter by Using a Search Query" on page 111

Creating a Filter by Using the Build Criteria Dialog

1. Log in to the Change Guardian Main interface.

   `https://<IP_Address/DNS_Change GuardianChange Guardian_server:8443>/sentinel/views/main.html`

   IP_Address/DNS_Change Guardian_server is the IP address or DNS name of the Change Guardian or server and *8443* is the default port for the Change Guardian server.
2. In the navigation panel, click **Filters** > **Create a filter**.
3. 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 4.

     For information on these parameters, see Table 13-1, "Build Criteria Dialog Box Elements," on page 108.
   - 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 4.

     For information about the syntax for the criteria, see Appendix A, "Search Query Syntax," on page 165.
4. (Conditional) If you do not want to include Change Guardian internal events in the search, select **Exclude system events**.
5. 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.
6. Review the search results to verify that the filter is retrieving the expected events.
7. (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.
8. When you are satisfied with the search results, click  , then click **Save as Filter**.
9. Specify a name for the filter and an optional description.
10. 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.

11 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 99.

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

- 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])
```

For more information on the search query syntax, see Appendix A, “Search Query Syntax,” on page 165.

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. For more information, see “The Default Search Field” in Appendix A, “Search Query Syntax,” on page 165.

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 Chapter 12, “Searching Events,” on page 93.

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.

14 LDAP 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.

Overview

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

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

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

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

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

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

Setting Up LDAP Authentication

Perform the following procedure to set up LDAP authentication:

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

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

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

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

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

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

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

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

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

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

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

  This is optional for eDirectory, and mandatory for Active Directory. For eDirectory, if the Base DN is not specified, the entire directory is searched to locate the users.

- **If Anonymous Search is No:** Specify the root container in the LDAP directory that contains the users.

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

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

For example:

- eDirectory:

  `uid`

- Active Directory:

  `sAMAccountName`

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

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

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

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

For example, test.example.com

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

On successful configuration:

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

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

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

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

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

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

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

Logging in by Using LDAP User Credentials

After you successfully configure the Change Guardian server for LDAP authentication, you can create Change Guardian LDAP user accounts. For more information on creating LDAP user accounts, see “Creating Users” on page 80.

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

15 Understanding Alerts

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

Overview

The following provides an overview of creating and monitoring alerts:

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

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

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

Managing Alert Rules

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

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

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

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

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

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

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

Creating an Alert Rule

When you create an alert rule, specify the following:

- The policy or policies that you want to be alerted on. If you do not specify one or more policies, the alert rule creates an alert for all events for all policies.
- An optional pattern the events must match before the alert rule creates an alert. For example, if you monitor the policy name for `DNS`, the alert rule creates alerts for all policies that contain `DNS` in the policy name, such as `DNS Configuration` and `Process and DNS`.
- Whether you want to be alerted on managed or unmanaged users.
- The event or events 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. If you do not specify the event name, the alert rule is applicable to all event names that satisfy the policy criteria.
- Whether you want to be alerted on success events or failure events.

  Additionally, you can monitor the following attributes:

  - InitiatorUserDomain: Domain name of the user who performed the event.
  - InitiatorUserName: Name of the user who performed the event.
  - ObserverHostName: The unqualified host name of the observing host.
  - ObserverIP: IP address of the observing host.
  - Severity: A normalized translation of the severity assigned to the event by the event source or to the alert by the event.
  - SourceHostDomain: The domain portion of the source host's fully-qualified host-name.
  - SourceHostName: The unqualified host name of the source host.
  - SourceIP: The IP address of the source host.
  - TargetHostDomain: The domain portion of the target host's fully-qualified host-name.
  - TargetHostName: The unqualified host name of the target host.
  - TargetUserName: The target user's account name.
- 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.

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

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

For more information about event destinations, see "Understanding Event Destinations" on page 49.

Redeploying Alert Rules

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

If you make changes to the alert rule, such as modifying its alert criteria or adding information to the knowledge base, you can redeploy it to the event destination. Redeploying an alert rule ensures the event destination has the most recent version of the alert rule. For more information about the alert knowledge base, see "Viewing Alerts" on page 122.

Ensuring Alternate Event Destinations Receive Alerts

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

1. Download the certificates from the 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. Open a command prompt and go to `/opt/novell/sentinel/bin`.
4. Run the following command for all alternate event destinations:

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

Managing Alerts

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

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

- Open an alert view and either pick an alert already assigned to them or claim an unassigned alert.
- View the alert details, such as the metadata, information about the alert rule that generated the alert, the triggering event and its identity information, and any knowledge base information associated with the alert.

- Determine the next step and add comments about the decision:
  - Close as harmless
  - Respond appropriately, and then close
  - Investigate further

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

Viewing and Triaging Alerts in Alert Views

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

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

Creating an Alert View

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

To create an alert view:

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

Viewing Alerts

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

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

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

To view alert views:

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

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

- Mouse over the charts to determine the number of alerts based on alert states, priority, and severity.
- Sort alerts based on one or more columns in the table. Press Shift+click to select multiple columns to sort. By default, the alert view table displays alerts based on the time when the alerts were triggered. Therefore, the latest alerts are listed on the top in the table.
- Assign alerts to a user or a role, including yourself or your role.
- Modify the alert state to indicate the progress on the alert investigation.
- Add comments to the alert to indicate the changes you made to the alert, which helps you to keep an up-to-date record of the alert investigation. For example, you can add comments when you change the state of a specific alert or when you have gathered more information about the alert. Providing specific comments allows you to accumulate knowledge about a particular instance of the alert and track how a particular condition was addressed. Comments are important in tracking the alert, particularly if the process of resolving the alert spans several users or roles.
- View events that triggered the alert and drill down further to the extent of viewing the user identities that triggered the event by clicking the **View details** icon in the alert view table.

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

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

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

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

  - **Alert Fields:** Displays the alert fields that provide the following information:
    - who and what caused the alert.
    - the assets affected.
    - the taxonomic categories of the action that caused the alert, the outcome, and so on. For more information on taxonomy, see Sentinel Taxonomy.
  - **Trigger Events:** Displays the events that triggered the correlated event associated with the alert. You can determine the conditions that triggered the alert by examining the trigger events.

- **Show history:** Displays the changes made to the alert, which helps you track any actions taken on the alert.
- **Identities:** Displays the list of users involved in the alert. This information helps you to investigate the users involved in the alert and monitor their activities.

Analyzing Alert Dashboards

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

Filtering Alerts

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

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

Creating an Alert Routing Rule

To create an alert routing rule to filter the alerts:

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

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

Ordering Alert Routing Rules

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

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

Configuring Alert Retention Policies

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

To configure the alert retention policy:

1. Log in to the Change Guardian web console.
2. Click **Storage > Alert**.
3. Specify the following:
   - The number of days from the date of creation of alerts, after which the alert status is set to closed.
   - The number of days from the date of closure of alerts, after which the alerts are deleted from Change Guardian.
4. Save the alert retention policy.

16 Visualizing and Analyzing Alerts

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. Correlation rules define the patterns that you are alerted to. Change Guardian automatically associates the relevant events and identities with the alert to help you determine the root cause of a potential threat.

Visualizing alerts helps you identify and analyze potential threats against your IT resources. Change Guardian provides graphical and tabular representations of alerts.

This chapter provides information about the following:

Viewing and Triaging Alerts

Change Guardian provides several ways to view alerts. 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 <Configuring Roles and Users>.

Change Guardian provides the following ways for you to view alerts in real time and triage them:

- **Threat Response Dashboard:** The Threat Response dashboard provides an overview of your current workload by breaking down alerts in groups, such as status, assignment, and priority. With the alerts grouped in this way, you can focus on and triage the high priority alerts assigned to you before triaging other alerts.

  To view alert details, click on any of the numbers or graphs.

  You can also:

  - Launch multiple pages in the browser
  - Share content with colleagues using a URL
  - Bookmark pages for quick access

NOTE: For users in the Operator role, the Threat Response dashboard is the main user interface for viewing and triaging alerts. Any user with permission to manage alerts can also use it. Users who wish to use alert views in the Change Guardian Main interface, or do not have permission to view or manage alerts on the Threat Response dashboard, can click Change Guardian Main in the left side navigation.

- **Alert Views:** In the Change Guardian Main interface, alert views provide a graphical and tabular representation of alerts that match the specified alert criteria. Charts provide a summary of alerts and the table provides high-level information about individual alerts. Change Guardian provides some alert views, but you can also create your own alert views and customize the alert criteria as necessary. For more information, see “Creating an Alert View” on page 129.

  To access alert views, click **Real-time Views** > **Alert Views**.

The alert table displays only distinct alerts. Duplicate alerts are rolled up to a single distinct alert. You can view the IP address of the remote Change Guardian server by moving the mouse over the name of the alert.

As you monitor alerts, you can perform the following activities:

- Mouse over the charts to determine the number of alerts based on alert states, priority, and severity.
- Sort alerts based on one or more columns in the table. Press Shift+click to select multiple columns to sort. By default, the alert view table displays alerts based on the time when the alerts were triggered. Therefore, the latest alerts are listed on the top in the table.
- Assign alerts to a user or a role, including yourself or your role.
- Modify the alert state to indicate the progress on the alert investigation.
- Add comments to the alert to indicate the changes you made to the alert, which helps you to keep an up-to-date record of the alert investigation. For example, you can add comments when you change the state of a specific alert or when you have gathered more information about the alert. Providing specific comments allows you to accumulate knowledge about a particular instance of the alert and track how a particular condition was addressed. Comments are important in tracking the alert, particularly if the process of resolving the alert spans several users or roles.
- View the events that triggered the alert and drill-down for more information. You can drill down to view the user identities that triggered the event by clicking the **View details** icon in the alert view table.

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

  - **Source / Background Information:** Displays the correlation rule that generated the alert. You can also annotate the correlation rule by adding information to the knowledge base so that future alerts generated by this correlation rule include the associated historical information.

    NOTE: In Change Guardian Main, the field is **Source**. In the Threat Response dashboard, the field is **Background Information**.

  - **Knowledge Base:** Knowledge base is a repository that contains information about the conditions that resulted in the alert. It can also include information about resolution of a particular alert, which can help others resolve similar alerts in the future. Over time, you can collect a valuable knowledge base about the alert specific to a tenant or an enterprise.

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

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

- **Alert Fields:** Displays the alert fields that provide the following information:
  - who and what caused the alert
  - the assets affected
  - the taxonomic categories of the action that caused the alert, the outcome, and so on.

  For more information about alert fields, click **Tips** on the top-right corner of the Change Guardian Main interface.
- **Trigger Events:** Displays the events that triggered the alert. You can investigate the conditions that triggered the alert by examining the trigger events. By default, the Alert Details page displays 10000 trigger events per alert. You can also define this number as necessary.

  To view the alert trigger events, click the **Search** icon.

  NOTE: Although the alert may include trigger events older than the configured data retention period, the search will display events that are within the data retention period.
- **Show history:** Displays the changes made to the alert, which helps you track any actions taken on the alert.
- **Identities:** (Change Guardian Main only) Displays the list of users involved in the alert. This information helps you to investigate about the users involved in the alert and monitor their activities.

NOTE: To perform more detailed analysis, you can use alert dashboards. For more information, see "Analyzing Alert Dashboards" on page 130.

Creating an Alert View

To view and analyze alerts in the Change Guardian Main interface, you must first create the alert view. To create the alert view, you must either be an administrator or have the Manage Alerts permission.

To create an alert view:

1. From **Change Guardian Main**, click **Real-time Views** > **Alert Views** > the **Create** icon.
2. Specify the following information:
   - **Name:** Specify a name for the alert view.
   - **Sharing:** Select either of the following options:
     - **Public:** Allow everyone to view the alert view. In the public mode, you are the owner of the alert view and other users cannot edit it.
     - **Private:** Only you will be able to view the alert view.
   - **Data sources:** Add other data sources from which you want to view alerts.
   - **Criteria:** Specify the criteria to filter the alerts.
   - **Tenant:** Select **All Tenants**, which is the default and recommended value.
   - **Time range:** Specify the time range for which you want to view alerts.
   - **Use alert period:** Select Created or Modified to view the alerts that were created or modified in the specified time range.
3. Click **Save** to save the alert view.

Analyzing Alert Dashboards

In the Change Guardian Main interface, alert dashboards allow you to analyze and study common patterns in alerts, such as:

- Types of alerts
- Average time owners take to close alerts
- The 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

You can create custom charts and tables for analysis. You can filter and refine the data further as you select certain areas in the charts and use the query and filter options.

For example, you are a Security Operations Center manager in a multi-tenant environment, and you want to analyze and investigate alerts in detail and also understand how your team is handling the alerts. You can perform the following analysis in the alert dashboard:

- **Investigate Alerts:** You can view the alerts generated over time, number of open alerts versus closed alerts, top correlation rules generating the most number of alerts, oldest open alerts, any spikes in alerts at a specific time range, and so on.
- **Monitor team performance:**
  - The type of alerts the team has been working on
  - How the alert load is distributed among top owners
  - Time taken to close alerts of specific priorities
  - Find the team member owning the most number of alerts
  - Team members that took longest to investigate alerts
- **Monitor performance against tenant service-level agreement (SLA):** You can view alerts from various tenants, analyze the most number of alerts from a specific tenant, time taken to investigate or close alerts for a specific tenant compared to other tenants, and so on.

The Alert dashboard provides a customizable and an easy-to-configure interface that helps you to view and investigate alerts in detail.

To create or view alerts in the dashboard, you must either be an administrator or have the permission to manage alerts. Depending on the alert permissions and the tenant you belong to, Change Guardian displays the relevant alerts in the dashboard.

Creating the Alert Dashboard

To create the alert dashboard:

1. In the Change Guardian Main interface, click **Dashboards** > **Alert** > click the **Create alert dashboard** icon.

   The Alert dashboard view opens in a new window. For information about analyzing alerts, see “Analyzing Alerts” on page 131.
2. (Optional) Customize the default dashboard to suit your requirements. For more information about customizing the alert dashboard, see “Customizing the Alert Dashboard” on page 131.
3. Click the **Save** icon to save the customized dashboard.

Analyzing Alerts

The Alert dashboard provides some pre-configured panels that provide information about alerts such as the following:

- **Overview:** Displays a time series chart that shows alerts generated in Change Guardian over time. You can inspect the time series charts for any spikes, which can indicate increase in attacks in your organization. You can drag and select the time period when the spike occurred to zoom into the alerts. As you select the specific time range, Change Guardian filters the dashboard for alerts in the selected time range. Also, you can find out the geographical locations from where the alerts originated.

  To view geographical locations from where the alerts originated, ensure that the `IpToCountry.csv` file is populated by using the IP2Location Feed plug-in.
- **Alert Load:** Provides information about the alerts at a granular level such as the following:
  - Topmost alerts in your enterprise
  - Alert distribution among top alert owners
  - Total number of alerts in individual alert states
  - Number of alerts received from each tenant
  - Total number of alerts based on priority
- **Performance rows:** Provides statistical information about how efficiently alerts are investigated and closed based on priority, correlation rule, alert owners, and tenants.
- **Details:** Provides detailed alerts information such as the oldest open alerts, number of times the duplicate alerts were rolled up, and all alert fields.

The alert dashboard displays all alerts in your local Change Guardian server. To view alerts from other Change Guardian servers, you need to view the alerts in the Alert Views. The alert dashboard displays only distinct alerts. Duplicate alerts are rolled up to a single distinct alert.

To view the alert dashboard:

1. In the Change Guardian Main interface, click **Dashboards** > **Alert**.
2. Select the desired alert dashboard and click the **Open alert dashboard** icon.
3. As you visualize and monitor alerts, you can perform the following activities in the alert dashboard:
   - Mouse over specific areas in the charts to view more information.
   - Select desired areas in the chart to filter the alert data. As you select a specific area in the chart, Change Guardian filters the alerts in rest of the charts and tables in the dashboard. Click **Filtering** to remove the applied filters and go back to the unfiltered view.
4. (Optional) You can customize the default view and save the dashboard. For information about customizing the dashboard, see “Customizing the Alert Dashboard” on page 131.
5. (Conditional) To perform various operations on alerts such as closing an alert, assigning alerts to a user, and so on, see “Viewing and Triaging Alerts” on page 127.

Customizing the Alert Dashboard

Change Guardian leverages Kibana, a browser-based analytics and search dashboard, that helps you to visualize and analyze data. The dashboard is divided into rows and panels. You can create rows and add panels as required to display various charts.You can drag and drop the rows or panels

to arrange them on the dashboard. You can also configure the size, style, and type of panels for a row. For more information, see rows and panels in Kibana documentation. As you visualize and monitor alerts, you can customize the alert dashboard as follows:

- Apply multiple filters to refine the alert data using the Query and Filter options. For more information about queries and filters, see queries and filters in Kibana documentation.
- Customize the rows and panels according to your requirements, for example, drag and drop the panels to arrange them on the dashboard. Click **Configure Dashboard** > **Rows** tab to arrange, create, or remove rows in the dashboard. For example, if you have to view the tenant specific information frequently, move the tenant performance row to the top or if you do not want to view the detailed tables, you can remove the Details row.
- Click the **configure** option in the panels to customize the size and style of panels.
- Add markers in the time series panel to display additional information such as owners, severity, and so on.

Troubleshooting

This section lists issues, which may occur when viewing alerts, along with the solution to resolve the issues.

Unable to View Alerts in the Dashboard and Alert Views

The alert dashboard and the charts in the alert view do not refresh or display new alerts. However, the table in the alert view displays the newly generated alerts. This issue could happen because of a corrupt alert index.

17 Understanding Agent Manager

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

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

  NOTE: You can roll back the updates.

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

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

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

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

Following are the different attributes in the Agent Manager console:

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

Understanding Asset Groups

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

Following are the different types of Asset Groups:

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

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

18 Backing Up and Restoring Data

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

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

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

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

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

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

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

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

- “Parameters for the Backup and Restore Utility Script” on page 136
- “Running the Backup and Restore Utility Script” on page 137
- “Restoring Data” on page 139

Parameters for the Backup and Restore Utility Script

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

Table 18-1 *Backup and Restore Script Parameters*

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

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

Running the Backup and Restore Utility Script

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

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

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

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

For more information on the different parameters, see Table 18-1. The following table lists examples of how to specify the parameters:

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

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

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

4 Use the Data Restoration feature to restore the extracted partitions. For more information, see “Restoring Data” on page 139.

Restoring Data

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

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

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

Enabling Event Data for Restoration

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

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

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

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

Viewing Event Data Available for Restoration

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

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

   The Data Restoration table chronologically lists all the event data that can be restored. The table displays the date of the event data, the name of event directory, and the location. The **Location** column indicates whether the event directory was found in the primary storage directory of Change Guardian or in the configured secondary storage directory.
4. Continue with "Restoring Event Data Where UID and GID are not the Same on the Source and the Destination Server" on page 140 to restore the event data.

Restoring Event Data

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

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

   The selected events are moved to the **Restored Data** section. It might take approximately 30 seconds for the **Restored Data** section to reflect the restored event partitions.
3. (Optional) Click **Refresh** to search for more restorable data.
4. To configure the restored event data to expire according to data retention policy, continue with "Restoring Data" on page 139.

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

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

To unsquash and squash the file system:

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

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

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

4 Unsquash the `index.sqfs` file:

```
unsquashfs index.sqfs
```

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

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

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

6 Remove the index:

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

7 Switch to novell user:

```
su novell
```

8 Squash the `squashfs-root` folder:

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

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

Configuring Restored Event Data to Expire

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

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

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

19 Configuring Data Federation

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

Overview

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

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

Configuring Servers for Data Federation

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

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

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

- "Enabling Data Federation" on page 144
- "Using the Administrator Credentials to Add a Data Source Server" on page 144
- "Using the Opt-in Password to Add a Data Source Server" on page 145

Enabling Data Federation

1. Create a role with **Proxy for Authorized Data Requestors** permission. For information on how to configure users and roles, see Configuring Roles and Users.
2. From Change Guardian Main as an administrator, click **Integration** > **Change Guardian**
3. Select **Local server and other data sources** in the **Data Sources** section.
4. Do one of the following to add data source servers to your authorized requestor:
   - If you are the administrator of the authorized requestor and you know the administrator user name and password on the data source server, continue with "Using the Administrator Credentials to Add a Data Source Server" on page 144.
   - If you are the administrator of the authorized requestor and you do not know the administrator user name and password on the data source server, you can set an opt-in password to allow administrators of data source servers to add their data source servers to the authorized requestor. Continue with "Using the Opt-in Password to Add a Data Source Server" on page 145.

Using the Administrator Credentials to Add a Data Source Server

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

IMPORTANT: You should ensure that the data source server that you add is able to communicate with the authorized requestor. The data source server should be able to communicate through TCP/IP. The IP address or host name of the data source server must be accessible through firewalls, NATs, etc. You can use the ping command to ensure that there is communication from both ways. If there is a communication failure between the servers, an error is displayed in the extended status page. For more information, see "Managing the Data Federation Search Results" on page 147.

---

1. If you are continuing from "Enabling Data Federation" on page 144, skip to Step 4; otherwise, continue to Step 2.
2. From Change Guardian Main as an administrator, click **Integration** > **Change Guardian**
3. Select **Local server and other data sources** in the **Data Sources** section.
4. Click the **Add a data source** link.
5. Specify the following information:

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

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

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

Password: Password associated with the user name.

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

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

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

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

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

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

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

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

8 Click **OK**.

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

You can now search events, view event reports, and view alerts from the data source server. For more information, see “Searching for Events” on page 147, “Running Reports” on page 149, and “Viewing Alerts” on page 149 respectively.

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

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

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

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

- “Setting the Opt-In Password” on page 146
- “Authorizing an Authorized Requestor Server” on page 146

Setting the Opt-In Password

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

   The Data Federation page that is displayed has two sections: **Data Sources** and **Authorized Requestors**.
3. In the **Data Sources** section, select **Local server and other data sources**.
4. Click **Set Opt-in Password**.
5. Specify the opt-in password, then click **Set Password**.
6. Continue with “Authorizing an Authorized Requestor Server” on page 146 to add the data source server to the authorized requestor.

Authorizing an Authorized Requestor Server

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

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

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

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

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

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

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

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

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

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

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

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

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

Searching for Events

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

1. Log in to the authorized requestor server as a user with Search Remote Data Sources permission.
2. Click **New Search**.
3. Click the **Data sources** link under the **Search** field.

   A dialog box is displayed that lists the data source servers that you have added, including the local server. The data source servers that are disabled are also displayed, but they are dimmed.
4. Select the check boxes next to the data source servers on which you want to perform a search, then click **OK**.
5. Specify the search criteria in the search field, then click **Search**.

   If you do not specify any search criteria, the authorized requestor server runs a default search for all events with severity 0 to 5.

   The Search Results page displays the events from the selected data source servers and the local server (if selected). The search results are filtered through the combination of the security filter and permissions of the logged-in user and the security filter and permissions of the search proxy role on the data source servers. For information on the distributed search results, see “Managing the Data Federation Search Results” on page 147.

Managing the Data Federation Search Results

The Search Results page displays the events from the selected data source servers and the local server, based on the search criteria you specified. Each event displays the data source server information from which the event is being retrieved.

You can expand the event results to see the details by clicking the **All** link.

For non-internal events, the **get raw data** link is displayed. You can view the raw data only if your role's security filter is set to view all event data.

NOTE: For search results that come from the data source servers, the role that is used to retrieve raw data is not the role of the logged-in user that is performing the search on the authorized requestor server, but the role that is assigned to the authorized requestor server on the data source server.

You can view the status of the search in the extended status page while a search is in progress as well as when the search has finished. To access the extended status page, click the **Displaying N of M events from X data sources** link that appears at the top of the refinement panel.

The extended status page displays the following information:

- **Data Source Name:** The descriptive name of the data source server. If you did not specify a descriptive name for the data source server, this field displays the IP address or DNS name of the data source server.
- **Events Available:** Indicates the number of events that have actually been retrieved from the data source server. The value is displayed as `N of M events available`, where N is the number of events that have been retrieved so far and M is the total number of events on the data source server that match the search criteria.
- **Retrieval Rate (EPS):** An approximate rate of how fast the events were retrieved from a specific data source server.
- **Status:** Displays the error messages, if any (generally in red). In addition to error messages, this field also displays the status of the search.
  - **Running:** Indicates that the search is still running on the data source server.
  - **Buffering events for display:** Indicates that the search is finished on the data source server, but the authorized requestor server is retrieving events from the data source server and buffering them for display.
  - **Paused buffering events for display:** Indicates that the search is finished on the data source server, and the authorized requestor has paused while retrieving events from the data source. The authorized requestor reads ahead a few pages from the last page that you scrolled down to. When it has buffered enough pages ahead, it pauses so that events are not buffered unnecessarily.
  - **Searching, paused buffering events for display:** This is similar to pausing and buffering events for display, except that the search is not yet complete on the data source server.
  - **Done buffering:** Indicates that the search is complete on the data source server, and all of the results are retrieved by the authorized requestor and queued for display.

Viewing the Search Activities

You can view the search activities that are being done on the data source server by the authorized requestor server. You can see what queries are being done and how frequently they are being done. Based on the search activity, you might want to assign a more/less restrictive proxy role or even disable access to the data source server.

You can also refine the search activity query. For example, you can change the date range to see what queries have been performed today or yesterday or in the last hour, or you can drill down to see the queries that were made by particular users on the authorized requestor.

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

   The Data Federation page that is displayed has two sections: **Data Sources** and **Authorized Requestors**.
3. In the **Authorized Requestors** section, a list of authorized requestor servers is displayed. Click the **Search Activities** link for the authorized requestor server for which you want to view the search activities.

   The search activities page is displayed that lists the audit events that are retrieved from all of the distributed search requests the data source server has received from that particular authorized requestor.

Running Reports

Running reports in a distributed environment is similar to running reports on your local server, except that you select the data source servers from which you want to view the reports while specifying the report parameters.

1. Log in to the authorized requestor sever as a user with Search Remote Data Sources permission.
2. From the Reports section, select the report you want to run, then click **Run**.

   The Run Report page is displayed.
3. Click the **Data sources** link.

   A page is displayed that lists the data source servers that you have added, including the local server. The data source servers that are disabled are also displayed, but they are dimmed.
4. Select the data source servers from which you want to view the reports, then click **OK**.
5. Specify the other parameters for the report.
6. Click **Run**.

   A report results entry is created and listed under the selected report.

Viewing Alerts

Viewing alerts in a distributed environment is similar to viewing alerts from your local server, except that you select the data source servers from which you want to view alerts while creating alert views.

To view alerts from data source servers, you must log in to the authorized requestor server as a user with Search Remote Data Sources permission.

Editing the Data Source Server Details

1. From Change Guardian Main as an administrator, click **Integration** > **Change Guardian**
2. In the **Data Sources** section, a list of data source servers is displayed under the Data Source Servers list.
3. Click the **Edit** link for the data source server for which you want to modify the details, then edit the information.

   You can edit the name of the data source server and the port number.
4. (Optional) To change the proxy role on the data source server as necessary:
   - **4a** Click **View/Change**.
   - **4b** Log in to the data source server.
   - **4c** Select a proxy role, then click **OK**.
5. Click **Save**.

Troubleshooting

You can perform some basic troubleshooting to ensure that you have successfully configured the authorized requestor for data federation. This section lists the most common issues and the probable causes for these issues.

Permission Denied

After doing a distributed search, check the extended status page to view the search status. If the search is not successful, check the following possible causes:

- The data source server administrator might have disabled data federation on the data source server. To enable data federation on the data source server, see Step 3 in “Authorizing an Authorized Requestor Server” on page 146.
- The data source server administrator might have disabled the authorized requestor server for data federation. Ensure that the authorized requestor server is enabled in the data source server. Fore more information, see “Authorizing an Authorized Requestor Server” on page 146.
- The role that you used for connecting might not have the `Search Data Targets` permission.

Connection Down

- Network issues in your organization.
- Change Guardian servers or Change Guardian services might be down.
- Connection time-out.
- The IP address or the port number of the data source server has changed, but the authorized requestor configuration might not be updated.

Unable to View Raw Data

The Proxy group that is assigned to the authorized requestor might not have the `view all events` permission to view the raw data.

Problems While Adding Data Source

The authorized requestor server and data source server might not be communicating with each other. Ensure that the firewall and NAT are set up properly to allow communication in both directions. Ping both ways to test.

Some Events Are Only Visible from the Local System

You might not be able to view the events from the data source servers for one of the following reasons:

- The trial license might be expired. You must purchase an enterprise license to reactivate this feature to view the events from the data source servers.
- The user who has logged in to the authorized requestor has one set of permissions on the local data such as view all data, view system events, security filter settings, and so on. The search proxy group has another set of permissions, possibly more restrictive. Therefore, certain types of data, such as raw data, system events, and PCI events, might be returned only from the local system and not the data source server.

Cannot Run Reports on the Data Source Servers

The trial license might be expired. You must purchase an enterprise license to reactivate this feature to run the reports from the data source servers.

Different Users Get Different Results

Different users might have different security filters or other permissions and therefore get different results from a distributed search.

Cannot Set the Admin Role as the Search Proxy Role

This is by design, for security reasons. Because the data viewing rights for the admin are unrestricted, it is not desirable to allow the admin role to be the search proxy role.

Error Logs

You can also determine the cause of a search failure by examining the log file on the authorized requestor server. The default location for the log file is `/var/opt/novell/Change Guardian/log`. For example, you might see one of the following messages:

```
Invalid console host name 10.0.0.1

Error sending target request to console host 10.0.0.1

Error getting certificate for console host 10.0.0.1

Authentication credentials in request to opt-in to console 10.0.0.2 were rejected

Request to opt-in to console 10.0.0.2 was not authorized

Error sending target request to console host 10.0.0.1
```

20 Upgrading Change Guardian

This chapter addresses planning considerations and provides a checklist to help you upgrade to the most current version of Change Guardian.

Change Guardian Upgrade Checklist

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

Table 20-1 *Upgrade Checklist*

	Tasks	See
❒	Ensure that the computers on which you install Change Guardian components meet the specified requirements.	Supported Platforms on the Technical Information page
❒	If you need to upgrade the operating system on the Change Guardian server, understand the recommended order for the upgrade.	“Planning an Operating System Upgrade” on page 154
❒	Review the supported operating system release notes to understand the known issues.	SUSE Release Notes
❒	Review the Change Guardian release notes to see new functionality and understand the known issues.	Change Guardian Release Notes
❒	Upgrade the Change Guardian server.	“Upgrading the Change Guardian server” on page 154
❒	Upgrade the Policy Editor.	“Upgrading Policy Editor” on page 157
❒	Upgrade the Windows Agent.	“Upgrading Windows Agent” on page 157
❒	Upgrade the Security Agent for UNIX	For information on how to upgrade Security Agent for UNIX remotely, refer to Security Agent for UNIX documentation.

Planning an Operating System Upgrade

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

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

Upgrading the Change Guardian server

You can upgrade the following installation types:

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

Upgrading a Traditional Installation

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

To upgrade the Change Guardian server in a traditional installation:

1. Back up all your information using the `backup_util.sh` script. For information about using the backup utility, see Chapter 18, “Backing Up and Restoring Data,” on page 135.
2. Download the latest installer from the Patch Finder website and copy it to the server. You must be a registered user to download patches. If you have not registered, click **Register** to create a user account in the patch download site.
3. Log in as `root` to the server where you want to upgrade Change Guardian.
4. Specify the following command to extract the install files from the tar file:

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

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

   ```
   ./install-changeguardian.sh
   ```
7. (Conditional) If you want to upgrade from a custom path, specify the following command:

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

    `https://IP_Address_Change_Guardian_server:8443`

Based on your requirement, you must perform the post upgrade tasks. For more information, see "Post-Upgrade Configuration for Change Guardian in FIPS mode" on page 156

Upgrading an Appliance Installation

To upgrade the Change Guardian server running as a managed software appliance, you can use zypper (a command line package manager).

When you want to update end user license agreement, you must upgrade the Change Guardian server appliance using zypper. For information about which methods of upgrade are supported for a release, see the Release Notes.

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

1. Back up your configuration and event information using the `backup_util.sh` script. For information about using the backup utility, see Chapter 18, "Backing Up and Restoring Data," on page 135.
2. Log in to the appliance as the `root` user.
3. To check for available updates, run the command `zypper lp`.
4. Install the updates by running the command `zypper patch`.

   WARNING: Always use the `zypper patch` command to update/upgrade the Change Guardian appliance. The `zypper up` command is not compatible with the Change Guardian appliance and might cause serious damage to your environment.
5. (Conditional) When prompted select **Solution 1** to downgrade `openssh`.
6. (Conditional) When prompted select **Solution 2** to change the architecture of `ncgContent`.
7. (Conditional) If a window asks you to resolve a merge conflict, select **Solution 1**.
8. Restart the Change Guardian appliance by running the command `reboot`.

For more information, see the zypper Cheat Sheet.

Based on your requirement, you must perform the post upgrade tasks. For more information, see "Post-Upgrade Configuration for Change Guardian in FIPS mode" on page 156

Disabling RC4 Communication

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

Perform the following steps to disable RC4 communication after upgrading:

1. Navigate to `cd /etc/opt/novell/sentinel/3rdparty/jetty`
2. Edit `jetty-ssl.xml`
3. Under the excluded cipher suites section, add the following ciphers:
   - SSL_RSA_WITH_RC4_128_SHA
   - SSL_RSA_WITH_RC4_128_MD5

4 Set the following attributes:

- **Owner**: Novell
- **Permissions**: 600

5 Restart services using `/opt/netiq/cg/scripts/cg_services.sh restart` command.

Post-Upgrade Configuration to Ensure Enhanced Keystore Security

Change Guardian now provides the `chg_keystore_pass.sh` script that allows you to change the keystore passwords. As a security best practice, you must change the keystore passwords immediately after upgrading to Change Guardian 5.0.

NOTE: You need not perform this procedure if Change Guardian server is in FIPS mode.

Perform the following procedure to change the keystore passwords:

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

2 Go to the `/opt/novell/sentinel/bin` directory.

3 Run the `chg_keystore_pass.sh` script and follow the on-screen prompts to change the keystore passwords.

Post-Upgrade Configuration for Change Guardian in FIPS mode

After you upgrade Change Guardian in FIPS mode, to ensure that Agent Manager works seamlessly, you must perform the post-upgrade configuration.

Perform the following tasks:

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

`./ams_cert_setup.sh --enable --profile=profile_ams`.

2 Back up the following file: `/opt/netiq/ams/ams/agent-manager.yml`.

3 Copy `/opt/netiq/ams/ams/security/profiles/profile_ams/agent-manager.yml` file to `/opt/netiq/ams/ams/` directory and ensure that you set user or group permissions `novell` user.

4 Rerun the FIPS conversion script on AMS. From a command prompt, change directory to `/opt/netiq/ams/ams/bin` and enter the following command:

`./convert_to_fips.sh`

5 Provide the requested input:

5a Create the password for the FIPS keystore database.

5b When asked whether to restart the Agent Manager service, select **y**.

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

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

Upgrading Policy Editor

The procedures for upgrading the Policy Editor is the same as the procedure for installing it. For more information, see “Installing the Policy Editor” on page 39.

Upgrading Windows Agent

You can upgrade Windows agent manually or using Agent Manager.

The procedures for upgrading the Windows agent 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. For more information, see “Manual Installation” on page 41.

To upgrade the Windows agents using Agent Manager:

1. From the assets list, select the an agent which you want to upgrade. You can select multiple computers if Agent Manager can use the same credentials to connect to the computers.
2. Provide credentials for an account that can connect to the computer and click **Next**.

   The account must be the local administrator account or a domain account in the Local Administrators group.
3. Click **Manage Installation**, and then select **Upgrade**.
4. Perform the following steps:
   1. For the agent version, select **Windows Agent *Agent Version***, where *Agent Version* is the version of the agent you want to deploy.
   2. Click **Start Upgrade**.

21 Uninstalling Change Guardian

This chapter includes the following sections:

Change Guardian Uninstallation Checklist

Use the following checklist to uninstall Change Guardian server:

- Uninstall the following components before you uninstall Change Guardian server:
  - Windows Agent and Security Agent for UNIX using Agent Manager
  - Policy Editor
- Complete the post-uninstallation tasks to verify the Change Guardian uninstallation.

Uninstalling Windows Agent

You can uninstall Windows agent in the following ways:

Remote Uninstallation Using Agent Manager

Use the following steps to uninstall the agent using Agent Manager:

1. Log in as `administrator` to the Change Guardian server.
   From Change Guardian Main, click **Integration** > **Agent Manager**.
2. Select the assets from which you want to uninstall the agent.
3. Select **Manage Installation** > **Uninstall Agents**.
4. Click **Start Uninstall**.

Manual Uninstallation

Use the following steps to uninstall the Windows Agent:

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

Uninstalling the Security Agent for UNIX

For information on how to uninstall Security Agent for UNIX remotely, refer to *Security Agent for UNIX* documentation.

Uninstalling Policy Editor

Use the following steps to uninstall the Policy Editor:

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

Uninstalling the Change Guardian server

To uninstall the Change Guardian server:

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

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

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

Post-Uninstallation Tasks

After you uninstall Change Guardian:

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

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

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

22 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.

Failed Installation Because of an Incorrect Network Configuration

Issue: During the first boot, if the installer finds that the network settings are incorrect, an error message is displayed. If the network is unavailable, installing Change Guardian on the appliance fails.

Workaround: To resolve this issue, properly configure the network settings. To verify the configuration, use the ifconfig command to return the valid IP address, and use the hostname -f command to return the valid hostname.

Change Guardian Main Interface is Blank in Internet Explorer After Logging in

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

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

Windows Agent Installation Using Change Guardian Agent Manager Fails

Issue: Windows agent installation using Change Guardian Agent Manager (CG AM) fails and displays the following error in failed task logs:

```
protocol negotiation failed...
```

This error might occur due to following reasons:

- SMB1 protocol is disabled on Windows agent.
- Change Guardian server is installed on SLES 11 SP4 or RHEL 6.7 platforms which supports SMBv1 only.

Workaround: Install Windows agent manually. For more information see “Manual Installation” on page 41.

Exception in the Change Guardian Logs When You Upgrade Change Guardian Versions from 4.2 or later to 5.0

Issue: When you upgrade Change Guardian appliance using zypper to 5.0 version, due to reconfiguration of the application you might see the following exception in the logs.

a) getKeyStore IOException : load failed `error while installing novell-SentinelSI-db-8.0.1.1-3611`

b) Warnings while installing `novell-Sentinelserver-8.0.1.1-3611`

```
WARNING: Failed to set encrypted password for property...
```

Workaround: Ignore the exception. There is no impact to Change Guardian functionality because of this exception.

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.

A Search Query Syntax

Change Guardian uses the Lucene query language for searching events. This section provides an overview of how to use the Lucene query language to perform searches in Change Guardian. For more advanced features, see Apache Lucene - Query Parser Syntax.

For information on the event fields in Change Guardian, click **Tips** on the top right corner in the Change Guardian Main interface. A table is displayed that lists the event names and their IDs.

Basic Search Query

A basic query is a search for a value on a field. The syntax is as follows:

`msg:<value>`

The field name (msg) is separated from the value by a colon.

For example, to search for a phrase that includes the word “authentication,” you can specify the search query as follows:

```
msg:authentication
```

Or, to search for events of severity 5, you can specify the search query as follows:

```
sev:5
```

If the value has spaces or other delimiters in it, you should use quotation marks. For example:

```
msg:"value with spaces"
```

Change Guardian classifies event fields as either tokenized fields or non-tokenized fields. A tokenized field is indexed and is searched differently than a non-tokenized field.

Case Insensitivity

Indexing and searching in Change Guardian is not case-sensitive. For example, the following queries are all equivalent:

```
msg:AdMin
msg:admin
msg:ADMIN
```

Special Characters

If you include special characters as part of a search, the special characters must be escaped. These characters are as follows:

```
+ - && || ! ( ) { } [ ] ^ " ~ * ? : \ /
```

Use “ \” before the character you want to escape. For example, to search for ISO/IEC_27002:2005 in the rv145 (Tag) field, use the following query:

```
rv145:ISO\/IEC_27002\:2005
```

You can also use quotation marks around the query:

```
rv145:"ISO/IEC_27002:2005"
```

If the value contains quotation marks, you must escape it by using the “\” character instead of quotation marks. For example, to search for “system “mail” service” in the `initiatorservicename` field, you must specify the query as follows:

```
sp:"system \"mail\" service"
```

For more information on quoting wildcard characters, see “Quoted Wildcards” on page 171.

Operators

Lucene supports AND, OR, and NOT Boolean operators, which allow words to be combined. Boolean operators must be always capitalized.

OR Operator

The OR operator is the default conjunction operator. If there is no Boolean operator between two clauses, the OR operator is used. The OR operator links two clauses and finds a matching event if either of the clauses is satisfied. The symbol || can be used in place of the word OR. For example, consider the following query:

```
sun:admin OR dun:admin
```

This query finds events whose initiator username or target username is “admin.” The following query produces the same result because OR is used by default:

```
sun:admin dun:admin
```

AND Operator

The AND operator links two clauses and finds a matching event only if both clauses are satisfied. The symbol && can be used in place of the word AND. For example, consider the following query:

```
sun:admin AND dun:tester
```

This query finds events whose initiator username is admin and the target username is tester.

NOT Operator

The NOT operator excludes events that match the clause after the NOT. The symbol ! can be used in place of the word NOT. For example, consider the following query:

```
sev:[0 TO 5] NOT st:I NOT st:A NOT st:P
```

This query matches all events whose severity is between 0 and 5, but excludes those whose sensor type is I (internal), A (audit), or P (performance); that is, it excludes Change Guardian internal events.

The NOT operator cannot be used by itself because it is a way to exclude events from a set that has been found by other search terms. For example, consider the following query:

```
NOT st:I NOT st:A NOT st:P
```

This query might seem like it should return all events where the sensor type is not I, A, or P. However, it is an invalid query because a query cannot begin with the NOT operator.

Operator Precedence

Parentheses can be used in the usual way to change operator precedence. They can be nested to any depth, as shown in the following examples:

```
(sun:admin OR dun:admin) AND (sip:10.0.0.1 OR sip:10.0.0.2)
```

```
((sun:admin OR dun:admin) AND (sip:10.0.0.1 OR sip:10.0.0.2)) OR (msg:user AND
evt:authentication)
```

The Default Search Field

Lucene uses a default search field, which is the field that is searched if no field is specified. In Change Guardian, `_data` is the default search field. By default, the default search field is a concatenation of the following event fields:

`evt,msg,sun,iuid,dun,tuid,sip,sp,dip,dp,rv42,shn,rv35,rv41,dhn,rv45,obsip,sn,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 (initiatorusername) and dun (targetusername). The sun field has the following value:

```
report-administrator
```

The dun field has the following value:

```
system-tester
```

The _data field contains the concatenation of these fields separated by a single space character:

```
report-administrator system-tester
```

Because the _data field is a tokenized field, the words “report,” “administrator,” “system,” and “tester” are indexed and searchable. The following queries would find this event:

```
report
```

```
_data:report
```

```
report-administrator
```

```
_data:report-administrator
```

```
report tester
```

In addition, the following queries also find this event:

```
sun:report-administrator
```

```
dun:system-tester
```

Tokenized Fields

Fields that are classified as tokenized fields are parsed into individual words for indexing. Therefore, a search occurs only on words within the field value. Characters that are considered to be word delimiters are not searchable, nor are words that are considered to be stop words. Lucene removes extremely common words to save disk space and speed up searching. These words are ignored in search filters. Currently, the following stop words are removed:

- a
- an
- and
- are
- as
- at
- be
- but
- by
- for
- if
- in
- into
- is
- it
- no
- not
- of
- on

- or
- such
- that
- the
- their
- then
- there
- these
- they
- this
- to
- was
- will
- with

When it does a search, Lucene examines all of the words in a field and tries to match words in the search value. For example, suppose that you specify a search for messages containing the following value:

```
msg:"user-authentication failed on the server"
```

The words that are parsed within this value are “user,” “authentication,” “failed,” and “server.” These are the only search words that would match this value. “On” and “the” are omitted because they are stop words.

The value has the hyphen character (-) between some words. Hyphens are treated as word delimiters, so Lucene does not search for hyphens. Consider, the following query:

```
msg:"user-authentication"
```

The results might not be exactly what you expect. The query search value matches the value, but not because it is matching the hyphen. It matches because Lucene first parses the words in the search value and identifies the words “user” and “authentication.” Lucene then matches those words against values that have the words “user” and “authentication” with no intervening words in between. This query would also match the following value, even though there is no hyphen between “user” and “authentication”:

```
user authentication has failed on the server
```

Consider the following query:

```
msg:"failed on server"
```

This query has the stop word, "on," which is ignored. However, the stop word does affect the relative positioning that is expected to be between words when evaluating a value to see if it matches. The “failed on server” search matches any phrase where the words “failed” and “server” are separated by exactly one word. It does not matter what the word is because the separating word is a stop word and is ignored. Thus, the above query would match all of the following:

```
failed on server
```

```
failed-on server
```

```
failed a server
```

```
failed-a-server
```

Proximity indicators created by using the ~ character followed by a value, make this more complicated. The query dictates an expected distance between words. In the “failed on server” query, the expected distance between “failed” and “server” is one word. The proximity indicator specifies how much variance there can be from the expected distance. For example, consider the following query, where a proximity indicator of one (~1) is specified:

```
msg:"failed on server"~1
```

This query indicates that the distance between “failed” and “server” could be plus or minus one from the expected distance, which is one because of the stop word “on.” Thus, the distance could be 1, 1-1 (0), or 1+1 (2). Thus, all of the following would match:

```
failed on server
```

```
failed on the server
```

```
failed finance server
```

As of Lucene version 3.1, word parsing is done according to word break rules outlined in the Unicode Text Segmentation algorithm. For more information, see Unicode Text Segmentation.

For information on tokenized fields in Change Guardian, in the Change Guardian Main interface click **Tips** on the top right corner of the Change Guardian Main interface. 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 171
- “Quoted Wildcards” on page 171
- “Leading Wildcards” on page 171

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" on page 171
- "Non-Tokenized Fields" on page 171

Tokenized Fields

When wildcards are quoted, they are not treated as wildcards, but as word delimiters. For example, consider the following query:

```
msg:"user* fail*"
```

The search value "`user* fail*`" is parsed into two words, "user" and "fail." The semantic is "find any event where the `msg` field contains "user" AND "fail" words in that order, and there are no intervening words between them." Thus, it does not match the following value:

```
The user authentication has failed on the server.
```

This is because the wildcard is not treated as a wildcard but as a word delimiter.

Non-Tokenized Fields

When wildcards are quoted, they are treated as literal characters to search. For example, if the query is: `sun:"adm*,"` it returns the following values:

```
adm*
```

```
ADM* (case-insensitive)
```

The query does not return the following values:

```
admin
```

```
ADMIN
```

Leading Wildcards

Leading wildcards are not valid in searches because Lucene does not allow the * or ? characters to be the first character of a search value. For example, the following queries are invalid:

- **sun:*adm*** The semantic is "find any event whose initiator username value contains the letters a, d, and m in sequence."
- **sun:*tester** The semantic is "find any event whose initiatorusername value ends with "tester."

- **sun:*** The semantic is “find any event whose initiator username field is non-empty.”

  Because this is an important type of query, Change Guardian provides an alternative way to accomplish this. For more information, see “The notnull Query” on page 172.

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 166.

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 174
- "Wildcards in IP Addresses" on page 174

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"
```