MICRO FOCUS®

# Change Guardian™

## User Guide for SaaS

**August 2023**

## Legal Notice

The only warranties for products and services of Micro Focus and its affiliates and licensors (“Micro Focus”) are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

For additional information, such as certification-related notices and trademarks, see http://www.microfocus.com/about/legal/.

# Contents

# About this Book and the Library

The User Guide for SaaS provides instructions about installing Change Guardian on CHA Appliance. This book also includes guidance for initial configuration to get you started.

## Intended Audience

This book provides information for administrators who are responsible for installing and administering the Change Guardian on-premises components.

## Additional Documentation

The Change Guardian documentation library includes the following resource:

**Online Help**

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

# 1 Introduction

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

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

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

This section provides information about the following:

- "What is Change Guardian?" on page 9
- "How Change Guardian Works" on page 10
- "Getting Started with Change Guardian Deployment" on page 14

## What is Change Guardian?

Change Guardian provides security intelligence to rapidly identify and respond to unauthorized activities of privileged users that indicate a security breach or compliance gaps. Change Guardian helps security teams to detect and respond to potential threats in real-time. Change Guardian achieves this by using intelligent alerting of authorized and unauthorized access, and helps detect changes to critical files, systems, and applications.

To manage sophisticated threats and complex computing environments, organizations must take a layered and integrated approach to defend their critical systems and sensitive data.

Change Guardian provides the following protection measures:

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

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

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

Change Guardian also integrates with your existing security information and event management (SIEM) solution. Change Guardian extends the ability of SIEM solutions to detect and respond to security incidents by providing information about who did what, when, where, and how, along with providing before and after values. With this comprehensive security intelligence, you can mitigate the impact of an attack before severe damage or compliance gaps can occur.

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

# How Change Guardian Works

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

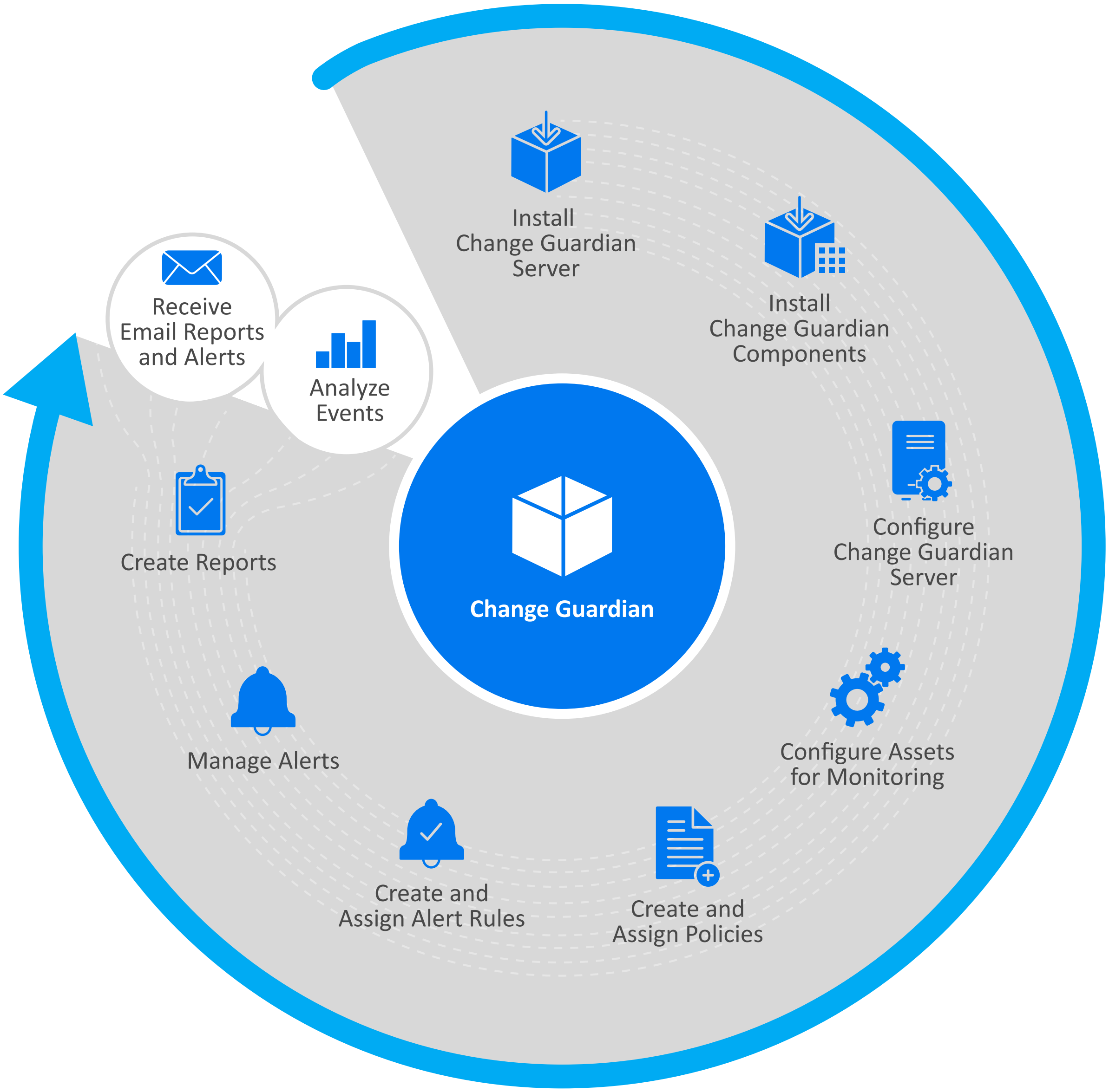
You can forward Change Guardian events to other software for further analysis and long term retention. You can forward events to another Change Guardian server, Sentinel server, Splunk Enterprise Security, or Micro Focus Security ArcSight Logger.

This section provides the following information:

- “Change Guardian Workflow” on page 10
- “Change Guardian in SaaS” on page 12
- “Top User Scenarios” on page 12

## Change Guardian Workflow

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

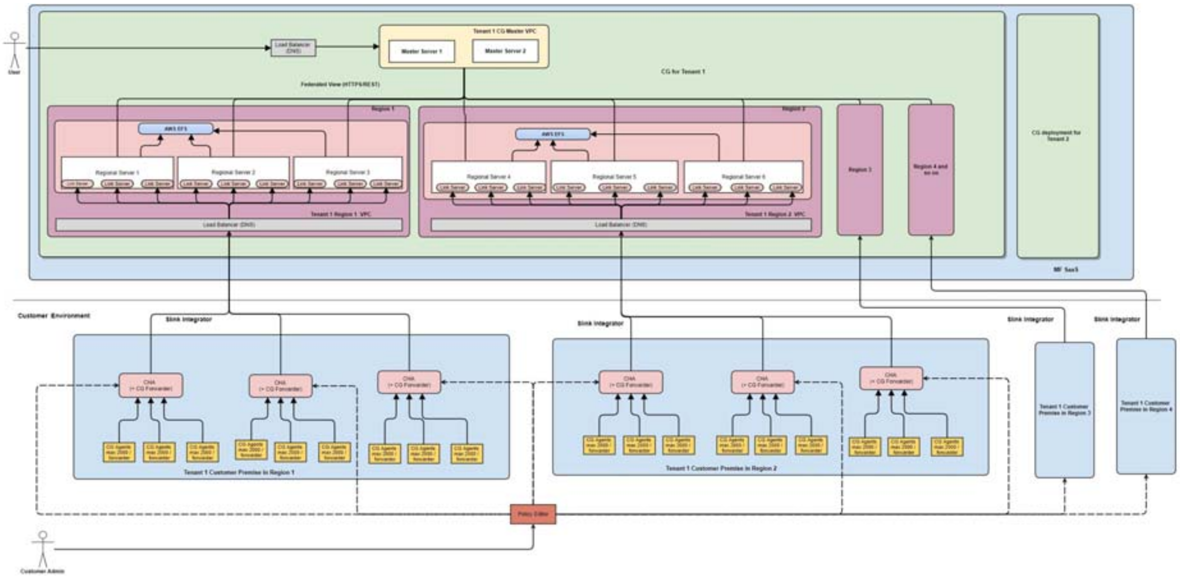


| Change Guardian Components | Description |
|---|---|
| Assets | Endpoints from where Change Guardian agents collect events. |
| Change Guardian Agents | Windows or UNIX based software that collects event data from the assets and forwards them to the Change Guardian server. |
| Change Guardian Server | A Linux-based computer that receives and stores the event data. The server also stores the policies that you create. You can also search for events, and create alerts and reports. |

| Change Guardian Components | Description |
|---|---|
| Agent Management | A central location where you can manage agents. You can deploy and manage your agents directly on the agent host machine, or remotely install agents using Agent Manager. |
| Policy Editor | A Windows-based console in which you can configure and manage policies, create and assign alert rules, configure event destinations, configure emails, and schedule monitoring. |
| Change Guardian Web UI | Interfaces to dashboards and management consoles where you can view event details and agent status, view and triage alerts, create event routing rules and alert routing rules, manage users, and so on. |

## Change Guardian in SaaS

The following diagram illustrates how Change Guardian works in a SaaS environment:



Change Guardian deployment in SaaS enables rapid monitoring of file system, application integrity, and system configuration. The Change Guardian server has been deployed in the SaaS environment and the Change Guardian server has been configured to work as a Forwarder that collects all the event data from the agents on the premise and sends the event data to the cloud.

## Top User Scenarios

- "Monitoring a Privileged User Account" on page 13
- "Monitoring Changes to File Integrity" on page 13
- "Adhering to a Standard Benchmark" on page 14

## Monitoring a Privileged User Account

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

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

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

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

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

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

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

## Monitoring Changes to File Integrity

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

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

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

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

### Adhering to a Standard Benchmark

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

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

## Getting Started with Change Guardian Deployment

Use this checklist to get started with Change Guardian deployment. Please complete the steps in the following order:

| Task | See |
|---|---|
| Review the hardware and software requirements, and the supported applications | Change Guardian System Requirements |
| Understanding the usage of ports for internal and external communication | Understanding Ports Used |
| Installing Change Guardian Forwarder on a physical CHA box | Installing Change Guardian Forwarder |
| Installing Change Guardian Forwarder on Cloud | Installing Forwarder on Cloud |
| Post Install Configuration of Connectors | Configuring Connectors |
| Enabling Event Data from various assets to Cloud | Enabling Event Data to Cloud |
| Windows, Linux, and UNIX Monitoring | Understanding Asset Monitoring |
| Understanding, creating, and assigning policies | Change Guardian Policies |

# 2 Preparing for Installation and Upgrade

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

- "System Requirements" on page 15
- "Security Considerations" on page 16
- "Understanding Application Licensing" on page 17
- "Understanding Ports Used" on page 17

## System Requirements

Micro Focus recommends the tested platforms listed below. However, customers running on any platforms not provided in this list or with untested configurations will be supported until the point Micro Focus determines that the root cause is the untested platform or configuration. Issues that can be reproduced on the tested platforms will be prioritized and fixed according to standard defect-handling policies. For more information about support polices, see Support Policies.

- "Software Requirements" on page 15
- "Recommended Hardware Requirements" on page 16

### Software Requirements

| Component Name | Platforms |
|---|---|
| **Change Guardian Forwarder** | ◆ ArcSight Connector Hosting Appliance with latest patches |
| **Change Guardian Policy Editor** | ◆ Windows Server 2022<br>◆ Windows 10 (64-bit)<br>◆ Windows Server 2019 |
| **Change Guardian Agent for Windows** | ◆ Windows Server 2022<br>◆ Windows 10<br>◆ Windows Server 2019 |

| Component Name | Platforms |
|---|---|
| **Change Guardian Agent for UNIX** | - Red Hat Enterprise Linux 9.2<br>- Red Hat Enterprise Linux 9.1<br>- Red Hat Enterprise Linux 9.0<br>- Red Hat Enterprise Linux 8.7<br>- Red Hat Enterprise Linux 8.6<br>- Red Hat Enterprise Linux 8.5<br>- Red Hat Enterprise Linux 8.3<br>- Red Hat Enterprise Linux 7.9<br>- IBM AIX 7.3<br>- Oracle Linux 8.7<br>- Oracle Linux 8.6<br>- Oracle Linux 8.5 |

### Recommended Hardware Requirements

| Component | Hardware |
|---|---|
| **Change Guardian Forwarder** | For information on the hardware specifications, refer Connector Hosting Appliance |

## Security Considerations

The following sections provide information about secured installations:

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

## Understanding Application Licensing

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

| Application Name | License Count |
|---|---|
| Windows | Number of monitored Windows servers or workstations |
| UNIX | Number of monitored UNIX, Linux, or UNIX-derivative servers or workstations |

## Understanding Ports Used

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

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

| Component | Ports | Direction | Required/ Optional | Description |
|---|---|---|---|---|
|  | TCP 8443 | Inbound | Required | Allows the Change Guardian server to receive events from monitored assets.<br>**NOTE:** This port might not be needed if you are sending events from monitored assets to an alternate destination. |

| Component | Ports | Direction | Required/ Optional | Description |
|---|---|---|---|---|
| Change Guardian Server | TCP 8077 | Outbound | Required | Allows the Change Guardian Server to connect to the Change Guardian Scanner service. |
|  | TCP 389 or TCP 636 | Outbound | Required | Enables the LDAP authentication and the expansion of Active Directory groups. The port initiates a connection to the LDAP server. |
|  | TCP 25 | Outbound | Optional | Default email port. This port may be different based on the specific email implementation. |
|  | TCP 1099 and 2000 | Inbound | Required | Used together by monitoring tools to connect to Change Guardian server process using Java Management Extensions (JMX). |
|  | TCP 5432 | Inbound | Optional. By default, this port listens only on loopback interface. | Used for the PostgreSQL database. |

| Component | Ports | Direction | Required/<br>Optional | Description |
|---|---|---|---|---|
| | TCP 8077 | Outbound | Required | Allows the Change Guardian Server to connect to the Change Guardian Scanner service. |
| | TCP 137, 138, 139, 445 | Outbound | Optional | Used if secondary storage is configured to CIFS. |
| | TCP/UDP 111 and TCP/UDP 2049 | Outbound | Optional | Used if secondary storage is configured to NFS. |
| | UDP 514 or TCP 1468 | Outbound | Optional | Used when Change Guardian forwards events to the system receiving Syslog messages. If the port is UDP, it sends a packet to the receiver. If the port is TCP, it initiates a connection to the receiver. |
| | TCP 32000 | | | Used for internal communication between the wrapper process and the server process. |
| | TCP 9200 | | | Used for communication with alert indexing service using REST. |
| | TCP 443 | Inbound | Optional | Forwarded to 8443 for HTTPS communication. |
| | TCP 61616 | Inbound | Optional | Used for incoming connections from Correlation Engines. |
| | TCP 8094 | inbound | Required | Allows the JAVOS service to accept connections from agents that are retrieving their assigned monitoring policies. |

| Component | Ports | Direction | Required/ Optional | Description |
|---|---|---|---|---|
| | TCP 9094 | Inbound (loopback) | Required | Allows the Change Guardian server to call JAVOS on this port to signal/reset the event destination cache. |
| | TCP 9095 | Inbound (loopback) | Optional | Allows users to see runtime metrics and active threads. |
| | TCP 8094 | Outbound | Required | Allows the agent to connect to the Change Guardian server to retrieve assigned monitoring policies. |
| | TCP 2620 | Inbound | Optional | Allows the Policy Editor to connect to the agent to browse objects on the monitored asset. |
| | TCP 8443 | Outbound | Required | Allows the agent to connect to the Change Guardian server to send events. |
| | TCP 8082 | Inbound | Required | Allows the agent to communicate with the Agent Manager. |
| | TCP 7443, 7444, 7445 | Inbound | Required | Used by the HTTP Server Connector. This port allows a Change Guardian server to receive events from Agents. |
| | TCP 1290, 1291, 1292 | Inbound | Required | This is the Sentinel Link port that is allowed to connect through the SuSE Firewall. |
| | TCP 10013 | Inbound | Required | Used by the Sentinel Control Center and Solution Designer. |

| Component | Ports | Direction | Required/ Optional | Description |
|---|---|---|---|---|
| **Change Guardian Agents** | TCP 445 | Outbound | Required | Allows the Agent Manager to deploy agents to Windows computers. |
| | TCP 22 | Outbound | Required | Allows the Agent Manager to deploy agents to UNIX computers. |

# 3 Installing Change Guardian Forwarder

The Forwarder is an on-premises component that can be used to manage agents and configure policies. It collects all the event data from the agents configured on the premise and sends the event data to cloud. This chapter guides you through installing the Change Guardian Forwarder on a physical CHA box.

## Setting Up Connector Host Appliance (CHA)

This appendix gives instructions on setting up your Connector Host Appliance for Change Guardian Forwarder for first use.

**Preparation:** Prior to first use of Connector Host Appliance, do each of the following:

1. Unpack the appliance and its accompanying accessories.
2. Read carefully through the instructions, cautions, and warnings packaged with the appliance. Failure to do so can result in bodily injury or appliance malfunction.
3. Note and save the rack-mounting instructions included in the package.
4. Redeem your Management Appliance license key. You will need this key to access Management Appliance functionality.
5. Follow the rack installation instructions (included in your Appliance package) to securely mount the appliance in its rack and make the back panel connections.
6. Do one of the following to enable local access to the Appliance:
   - Connect a keyboard, monitor, and mouse to the ports on the Appliance.
   - Connect a terminal to the serial port on the Appliance using a null modem cable with DB-9 connector. The serial port requires a standard VT100-compatible terminal: 9600 bps, 8-bits, no parity, 1 stop bit (8N1), no flow control.
7. Power on the appliance.
8. Optionally, enable your appliance for out-of-band remote access. Download, review, and follow the instructions in the ProLiant Integrated Lights-Out User Guide, available on the product's website.

You are now ready to begin appliance set up.

## Set Up

During appliance setup, do the following:

1. Configure a new IP address for the appliance at the CLI.
2. Accept the End User License Agreement, then log in to the appliance.
3. Initialize the CHA Management Centerappliance.

Each of these steps is described in detail below.

## Configure a New IP Address

Use the appliance's Command Line Interface (CLI) to configure a new IP address. CHA Management Center Appliance ships with the default IP address 192.168.35.35 (subnet mask 255.255.255.0) on Eth0. You will also need to specify a default gateway, hostname, and DNS and NTP servers.

You will need the following information on hand before beginning:

- The new IP address , plus prefix or subnet mask
- Your default gateway address.
- Your fully-qualified domain name.
- One or more name search domains and server addresses for DNS resolution.
- One or more NTP server addresses.

### To configure a new IP address on the CLI:

1. On the CLI, connect to the appliance using these default credentials:

   **Login: admin**

   **Password: password**

2. Specify the new IP address with one of the following commands:
   - `set ip eth0 <ip>/<prefix>, where <ip> is the new IP address and <prefix> is your prefix, OR,`
   - `set ip eth0 <ip> <subnetmask>, where <ip> the new IP address and <subnetmask>` is your subnet mask
3. Specify `set defaultgw <address>`, replacing `<address>` with your default gateway IP address
4. Specify `set hostname <FQDN>`, replacing `<FQDN>` with the fully-qualified domain name of the host.
5. Specify `set dns <search_domain_1>`, `<search_domain_2>...<search_domain_N> <nameserver1> <nameserver2>...<nameserver_N>`, replacing each `<search_domain_N>` with a search domain, and each `<nameserver_N>` with the IP address of a nameserver you wish to use for DNS.
6. Specify `set <ntp_server_1> <ntp_server_2>...<ntp_server_N>`, replacing each `<ntp_server_N>` with the IP address of an NTP server you wish to set appliance time.

7. Specify `show config` and review your settings. If any are incorrect, correct them as described in earlier steps.

   You are now ready to accept the End User License Agreement.

### Accept the End User License Agreement

Upon first connecting to the appliance through a browser, you are prompted to accept the End User License Agreement (EULA).

***To accept the EULA:***

1. In a browser, connect to the CHA Management Center appliance at https://<IP>, where <IP> is the new IP address you just configured.
2. Review the license.
3. Select the I accept the terms of the License Agreement check box, then click Accept.
4. Log in as an administrator using the default credentials.

   **Login:**admin

   **Password:**password

   You may now initialize the appliance.

### Initialize the CHA

You can now initialize the appliance by uploading the license file; optionally, setting date and time settings; and then changing the admin login credentials to non-default values.

***To initialize the appliance:***

1. On the CHA Management Center Appliance Configuration page, in the License field, browse for and upload your current license.
2. Click Save.
3. Set your date and time settings for the appliance.
4. Change the admin login credentials from their default values. For instructions, see Change Password.

   Your CHA appliance is now ready for use.

## Installing Change Guardian Forwarder

This section provides information on the following:

- "Prerequisites" on page 26
- "Getting Started" on page 26
- "Installing Change Guardian" on page 28

## Prerequisites

To begin with the installation of the Forwarder, download the following files on the specified machines:

**Download on Windows**:

1. **pe_prerequisite.zip**
   - DotNet_Runtime_5.0.17
2. **cha_prerequisite.zip**
   - ArcMC_3.1
   - ArcMC_3.1.2
   - Connector_8.3.0P2
   - osupgrade_rhel79_202205
3. **Production License Key**
   - CG-licfile.xml

**Copy to Forwarder**:

---

**NOTE:** To copy the downloaded files to Forwarder, ensure that you have enabled SSH. To know more, see Enable SSH Configuration.

---

1. **change_guardian_installer_6211.zip**
   - change_guardian_prerequisite_configuration_6211
     - change_guardian_prerequisite_configuration_6211.sh
2. **change_guardian-6.2.1.1.tgz**

## Getting Started

Once you have downloaded all the prerequisite files in the appropriate machines, perform the following steps in each of the forwarder boxes for the installation of Forwarder:

- "Enabling SSH Configuration" on page 26
- "Updating Operating System" on page 27
- "Upgrading CHA" on page 27
- "Upgrading Connector to 8.3 Patch 2" on page 28

---

**NOTE:** The following steps are to configure a single CHA box. To configure more boxes, apply the same steps to the other CHA boxes as well.

---

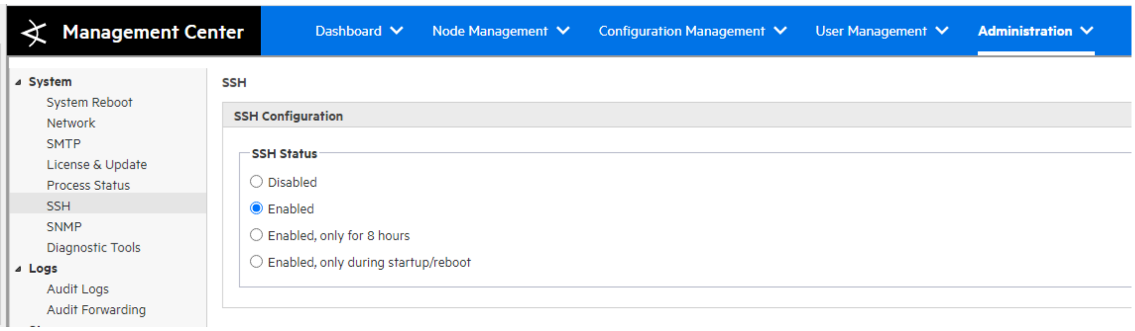
### Enabling SSH Configuration

1. Login to *Change Guardian Management Center* using the following URL:

   `https://<hostname or IPaddress>:<configured_port>`. The default port is 443.
2. To login for the first time, use the following default credentials:

```
Username: admin
Password: password
```

3. When prompted, change the default password to a new password.
4. From the *Change Guardian Management Center* home page, click **Administration** > **System Admin**.
5. Select **SSH** from the **System** list.



SSH

SSH Configuration

SSH Status

○ Disabled
● Enabled
○ Enabled, only for 8 hours
○ Enabled, only during startup/reboot

6. Set the **SSH Status** to **Enabled**.

## Updating Operating System

1. Click **Administration** > **System Admin** from top-level menu bar.
2. Click **License & Update** in the **System** section.
3. Click **Browse** and locate the extracted folder `osupgrade_rhel79_202207`.
4. Select the file `<Extract location>\cha_prerequisite\osupgrade_rhel79_202205\osupgrade-arcmc-rhel79_202207_202208012306.enc`.
5. Click **Upload Update**. The **Update In Progress** page displays the update progress.
6. Once the update has completed, the **Update Results** page displays the result as success or failure and whether the update requires a reboot. If the update requires a reboot, the Arcsight Management Center reboots automatically.

## Upgrading CHA

1. **Upgrading CHA 3.0.0 to 3.1.0:**
   - Click **Administration** > **System Admin** > **License & Update**.
   - Click **Browse**. Locate the extracted folder `ArcMC_3.1` and select the file `<Extract location>\cha_prerequisite\ArcMC_3.1\arcmc-2266.enc`
   - Click **Upload Update**. An **Update In Progress** page displays the update progress.
   - Once the upgrade is finished, restart ArcMC.
2. **Upgrading CHA 3.1.0 to 3.1.2**:
   - Click **Administration** > **System Admin** > **License & Update**.

- Click **Browse**. Locate the extracted folder `CG_3.1.2` and select the file `<Extract location>\cha_prerequisite\ArcMC_3.1.2\arcmc-2288.enc`
- Click **Upload Update**. An **Update In Progress** page displays the update progress.
- Once the upgrade is finished, restart CHA.

## Upgrading Connector to 8.3 Patch 2

To upgrade the connector, upload the version file to repositories and then upgrade all the connectors in a container.

1. Select CHA repository by clicking **Administration** > **Repositories**.
2. Select **Upgrade Files** from the navigation tree.
3. Click **Upload** in the management panel.
4. Click **Choose File** and browse to your connector AUP file `<Extract location>\cha_prerequisite_installers\Connector_8.3.0P2\ArcSight-8.3.0.8731.2-Connectors.aup`.
5. Click **Submit**. The version file is uploaded.
6. Click **Node Management**.
7. In the navigation tree, navigate to the host on which the container resides and click the **Containers** tab.
8. On the **Containers** tab, select one or more containers to upgrade and click **Upgrade**.
9. Select **Framework upgrade** under **Select Upgrade Type** on the upgrade page.
10. Select version 8.3.0.8731.2 from the **Select Upgrade Version** drop-down list to upgrade the selected containers.

    **NOTE:** For a parser upgrade, if the selected parser version is from the Marketplace and not the local repository, save your Marketplace credentials in CHA. This is a one-time task unless you wish to update these credentials.

11. Click **Upgrade**. The upgrade is performed on all containers.

# Installing Change Guardian

Perform the following steps to install Change Guardian server:

## Prerequisites

- Copy the following zip file to the forwarder machine:

  `change_guardian_installer_6211.zip`. Extract the zip file.
- Navigate to `change_guardian_installer_6211/`. Select the folder `change_guardian_prerequisite_configuration_6211/` and run the following command:

  ```
  chmod +x change_guardian_prerequisite_configuration_6211.sh
  ```

- Run the following script:

  ```
  change_guardian_prerequisite_configuration_6211.sh
  ```

## Installing Change Guardian Server

**NOTE:** Post installation, if you change the IP address of the Connector Host Appliance server, there is a breakdown of communication between the Change Guardian server and agent. This requires reconfiguration of the server to restore communication. Therefore, consider using static IP addresses in your Connector Host Appliance.

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

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

2. Create a Change Guardian directory in `/opt/arcsight/connectors path`

   ```
   mkdir /opt/arcsight/connectors/changeguardian
   chmod 0755 /opt/arcsight/connectors/changeguardian
   ```

3. Navigate to the extracted folder `change_guardian_installer_6211/` in the forwarder machine.

4. To install from a custom path, specify the following command:

   ```
   ./install-changeguardian.sh --location=/opt/arcsight/connectors/
   changeguardian
   ```

   **NOTE:** This custom path must have 0755 permissions. Ensure that you allocate the recommended disk space in / and /home.

5. (Conditional) If NTP could not synchronize your computer time with the network time, make the required changes to the computer.

6. (Conditional) If your system does not meet the recommended disk space, make the required changes to the computer.

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

8. Read the license agreement completely before you accept it. You may press the space bar to scroll through the complete agreement.

9. When prompted, select the standard configuration.

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

    **NOTE:** While setting the admin password, all non-alphanumeric characters are allowed to be used to set the password.

11. When prompted **Do you want the Change Guardian agents to locate this system by IP address or by host name?**, Select default choice [1] if the Connector Host Appliance is configured with static IP Address.

12. When prompted **Please enter your Sentinel admin password**, enter the password created for admin account in step 10.

13. Create a password for the cgadmin user.

14 Select ‘n', when prompted **Configure a default email destination**.

15 After the completion of Change Guardian server installation, it might take a few minutes for all services to start. Wait until the installation finishes and starts all services before you log in to the server.

**NOTE:** You can also configure email servers by using the server command prompt. For more information, see Configurations using the Server Command Prompt.

# Installing Change Guardian Forwarder on Cloud

Change Guardian Forwarder is deployed and configured on cloud to receive events from agents that are configured on cloud. It also forwards the event data to regional instances. To install a Forwarder on cloud, ensure that you perform the following steps in all the regions that will be using the Forwarder:

1 Login to AWS console and deploy a RedHat 7.9 instance by navigating to **EC2** > **Images** > **AMIs**. Select **Public Images** and use the filters below to find the latest image:

- AMI name: RHEL-7.9_HVM-*
- Architecture: x86_64
- Virtualization: hvm
- Root device type: ebs
- Owner: 309956199498

2 Additionally, you can also choose the following during deployment:

- Instance type: m5.4xlarge
- Disk with a minimum storage space of 1 TB
- Ports can be used during the creation of security groups. For more information on ports, see Understanding Ports Used.

3 Installing Change Guardian

- Ensure that all the Change Guardian prerequisites are met. For information on the prerequisites, see Installing Change Guardian.

  **NOTE:** For additional package installation, you might require a RedHat Subscription.

- It is recommended to configure Change Guardian with a private IP address. Post installation, if you change the IP address of the cloud forwarder machine, the communication between Change Guardian server and agents gets disrupted. To restore the communication, you need to reconfigure the server.
- Download the Change Guardian installation file from the Downloads website. Copy to the cloud forwarder instance.
- On the command line, log in as the root user and type the following command to extract the installation file:

  ```
  tar -zxvf change_guardian-<version>.tgz.
  ```
- Run the Change Guardian server installation program as root by typing the following command in the root of the extracted directory:

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

**NOTE:** Ensure that you allocate the recommended disk space in / and /home.

- (Conditional) If NTP could not synchronize your computer time with the network time, make the required changes to the computer.
- (Conditional) If your system does not meet the recommended disk space, make the required changes to the computer.
- Specify the language as English, then press **Enter**. The end user license agreement is displayed in the selected language.
- Press the space bar to read the license agreement. You must scroll through the entire agreement before you can accept it.
- When prompted, select the standard configuration.
- Create an admin account password for global system administration.

**NOTE:** While setting the admin password, all non-alphanumeric characters are allowed to be used to set the password.

- When prompted **Do you want the Change Guardian agents to locate this system by IP address or by host name?**, Select default choice **[1]** if the Connector Host Appliance is configured with static IP Address.
- When prompted **Please enter your Sentinel admin password**, enter the password created for admin account.
- Create a password for the cgadmin user.
- Select ‘n', when prompted **Configure a default email destination**.
- After the completion of Change Guardian server installation, it might take a few minutes for all services to start. Wait until the installation finishes and starts all services before you log in to the server.
- To verify the installation, see Verifying the Installation.

# Verifying the Installation

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

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

  The possible *port_number* are 8443, 8094, 8082, and 2620. For example, running the command with ports 8443 might provide the following output:

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

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

  For more information about the ports used, see Understanding Ports Used.

- Access the Change Guardian dashboard:

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

# 4 Installing Change Guardian Components

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

**Policy Editor:** Allows you to configure Change Guardian policies. The Policy Editor runs on a supported Windows machine.

**Change Guardian Agent for Windows:** Collects event data for the supported assets such as Windows.

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

---

**NOTE:** The event caching for Windows and UNIX agents is set to 10MB. When the communication between agent and forwarder is disrupted, the agent can store events up to the cache size.

---

For information about requirements and recommendations, see System Requirements.

This chapter provides the following information:

## Installing Policy Editor

### Prerequisites:

- Install .Net Core Runtime Framework 5.0. To install the framework, download the `pe_prerequisite.zip` file.

### To install Policy Editor:

1. In the web console, click **AGENTS**.
2. In Agent Manager, click **All Assets > Manage Installation > Download Package**.
3. Download the available version of Policy Editor on your Windows machine.
4. Copy the `ChangeGuardianPolicyEditor.zip` file to the computer where you want to install Policy Editor and extract the files.

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

## Verifying the Installation

To verify:

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

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

# Installing Change Guardian Agent for Windows

**Prerequisites**: Using Agent Manager, add the assets where you want to install agents. You can either import assets from Active Directory or from a text file, or add assets manually. For more information, see Adding Assets.

- "Adding Assets" on page 34
- "Installing Change Guardian Agent for Windows:" on page 35
- "Verifying the Installation" on page 37

## Adding Assets

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

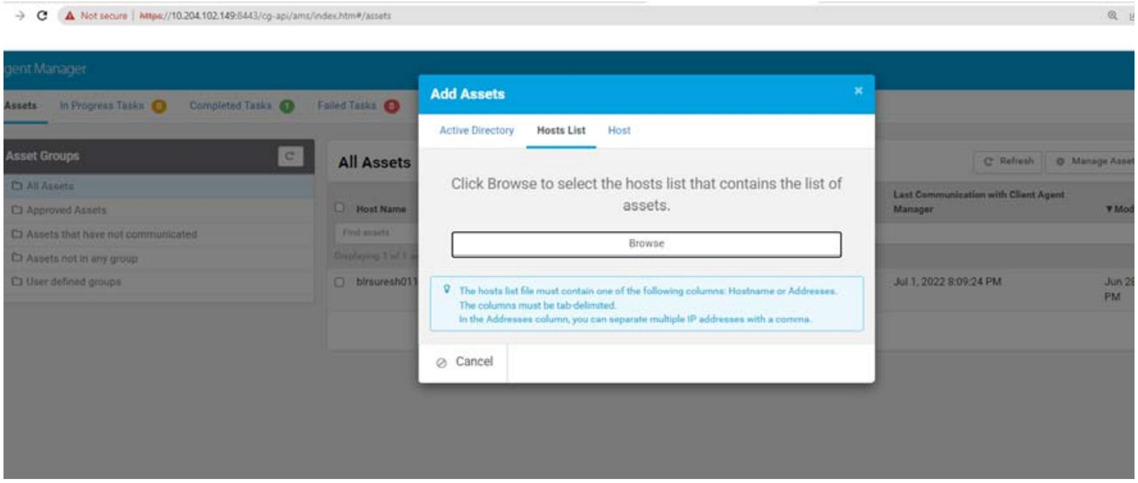
An **asset group** is a set of assets or devices that you want to associate with one another. Each asset group can contain assets, another asset group, or a combination of assets and asset group. Asset groups allow you to assign policies to the group instead of to each individual computer. When you add an asset to a group, Change Guardian automatically deploys the policies assigned to the group to the new asset.

**To add assets:**

1. Open the following URL:

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

   The default port is 8443. You can use a custom port if Change Guardian was installed with custom configurations.
2. In the web console, click **AGENTS**.
3. Click **All Assets > Manage Assets > Add**.



Click Browse to select the hosts list that contains the list of assets.

The hosts list file must contain one of the following columns: Hostname or Addresses.
The columns must be tab-delimited.
In the Addresses column, you can separate multiple IP addresses with a comma.

**4** (Conditional) To import assets from an Active Directory server, use the **Active Directory** tab.

**NOTE:** If you are using Active Directory over SSL or TLS connection, ensure that you have imported the Active Directory SSL certificate to the Change Guardian server. For more information, see "Using CA Signed Certificates" on page 71.

**5** (Conditional) To import assets from a text file, use the **Hosts List** tab.

Create a text file with a header line containing the columns Hostname, MajorType, and Addresses, and use a tab to separate the columns. In the Hostname column, specify the fully-qualified domain names of the computers where you want to deploy agents. Optionally, you can specify the IP addresses under the Addresses column. In the MajorType column, specify whether the operating system is UNIX or Windows.

**6** (Conditional) To manually add an asset, use the **Host** tab.

You can move an asset from one group to another:

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

## Installing Change Guardian Agent for Windows:

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

- Remote Installation
- Manual Installation

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

## Remote Installation

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

**Prerequisite**: Using Agent Manager, you must first add the assets where you want to install agents. You can either import assets from Active Directory or from a text file, or add assets manually.

**To install:**

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

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

4. Select the available version of the agent.
5. For agent configuration, select any one option: default agent configuration, customize the configuration, or add new.
6. Click **Start Installation.**

## Manual Installation

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

- "Downloading the Agent Certificates and Artifacts" on page 36
- "Installing the Agent" on page 36

### Downloading the Agent Certificates and Artifacts

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

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

**To download:**

1. In Agent Manager, click **All Assets > Manage Installation > Download**.
2. Select the **Agent certificates and artifacts** package.
3. Specify the hostname and the IP address, and then click **Start Download**.
4. Copy and extract the `ChangeGuardianAgentCertificates_<`*`hostname`*`>.zip` file to the agent artifact directory, before installing the agents.

### Installing the Agent

**To install:**

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

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

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

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

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

## Verifying the Installation

To verify:

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

# Installing Change Guardian Agent for UNIX

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

- "Interactive Installation" on page 37
- "Silent Installation" on page 38
- "Validating the Installation" on page 40

## Interactive Installation

This section provides the following information:

- "Remote Installation" on page 37
- "Manual Installation" on page 38

### Remote Installation

**To install:**

1 In Agent Manager click **Asset Groups > All Assets > Manage Assets > Add**.

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

3 Click **Manage Installation > Install Agents**.

4 Provide the `remote user` credentials of the machine and click **Next** and start the installation. (The remote user could be root or any other user with permission to run commands with elevated privileges and must have SSH access enabled.)

If you select multiple machines, ensure that the `remote` users shares the same password.

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

### Manual Installation

**To install:**

1 Download the agent artifacts and certificates. For more information, see "Downloading the Agent Certificates and Artifacts" on page 36.

2 Log in to the machine where you want to install the agent, as a remote user (root or any other user with permission to run commands with elevated privileges) and with SSH access enabled.

3 Click **All Assets > Manage Installation > Download**, and download the required package.

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

4 Extract `ChangeGuardianAgentForUnix.zip` to the computer where you want to install the Change Guardian Agent for UNIX.

5 Provide file execute permission to the `./install.sh` file and execute the `./install.sh` script.

6 Follow the prompts to complete the installation.

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

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

## Silent Installation

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

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

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

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

**To install:**

1. Download the installation files from the Downloads website.
2. Log in to the machine where you want to install the agent as a remote user (root or any other user with permission to run commands with elevated privileges) and with SSH access enabled.
3. Download and extract the install files from the tar file using the following command:

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

   Replace *<install_filename>* with the actual name of the install file.
4. After you create the installation file, you can run silent installation on the endpoints from command line using the following command:

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

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

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

| Parameter | Description |
|---|---|
| FRESH_INSTALL | Specifies whether you want to install or upgrade the agent. Valid entries are 1 (install) and 0 (upgrade). The default value is 1. |
| CREATE_TARGET_DIR | Specifies whether you want the install program to create the target installation directory if it does not already exist. Valid entries are y and n. The default value is y. |
| CONTINUE_WITHOUT_PATCHES | Specifies whether the install program stops or continues when the operating system is not a supported version. Valid entries are y and n. The default value is n. |
| IQ_STARTUP | Specify restart method for the agent process. For information about the options, see "Validating the Installation" on page 40. Valid entries are rclink and inittab. The default option is rclink. |
| CGU_STARTUP | Specifies restart method for the detected process. For information about the options, see "Validating the Installation" on page 40. Valid entries are rclink and inittab. The default value is rclink. |
| MANAGE_AUDIT_LOGS | Specifies whether the agent reduces the size and removes old audit logs. Valid entries are y and n. |
| AUDIT_LOG_SIZE | Specifies the maximum size, in bytes, that the agent allows an audit log to reach before starting a new log. |

| Parameter | Description |
|---|---|
| AUDIT_LOG_RETENTION | Specifies the number of audit logs that the agent keeps. Once this number of audit logs exists, the agent deletes old logs when making new ones. |
| KEEP_OLD_AGENT_DIR | Specifies whether to keep the previous installation directory when you are upgrading the agent. Valid entries are y and n. |
| OLD_INSTALL_DIR_MOVED | Specifies the directory where you want the installation program to move to the previous installation directory. |

## Validating the Installation

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

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

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

  The output in Linux is as follows:

  ```
  root 10447 1 0 14:39 ? 00:00:00 /usr/netiq/common/bin/nqmagt -g /usr/
  netiq/common/log/nqmagt.log
  root 10449 10447 0 14:39 ? 00:00:02 VigilEntAgent -config vigilent -
  load va:VigilEntAdapter -d
  root 135 2 0 Nov01 ? 00:00:41 [kauditd]
  root 6133 1 0 Nov01 ? 00:03:12 /sbin/auditd
  root 10358 1 0 14:39 ? 00:00:00 ./perl - ../local/cache/detect.xml vrun
  detectd
  root 10430 10358 0 14:39 ? 00:00:00 detectd[10358] -p local4.err
  root 10445 10358 0 14:39 ? 00:00:00
  detect_group:LinuxAuditObject__singleton
  root 9830662 1 0 02:01:56 -0:07 /usr/netiq/cam/bin/nq_cam
  ```

- `detectd`: Monitors tasks and retrieves data.
- `vigilent`: Sends events to the Change Guardian server.
- `auditd`: Writes audit records to the disk. It is an operating system service that is required by the services specific to Change Guardian Agent for UNIX. If `auditd` is not running, follow the operating system instructions to enable it.
- `nqmagt`: Monitors the status of the other agent processes and restarts them if necessary. This process should run continuously after the agent is installed.
- nqcam: The Client Agent Manager Service executes the UNIX Agent reconfigure/ upgrade/ uninstall tasks.
- To validate in Linux platforms, check if the agent services `vigilentagent.service`, `detectd.service` and `nq_cam.service` are running:

  ```
  systemctl status <service_name>
  ```

  Where *service_name* can be `nq_cam.service`, `vigilentagent.service`, or `detectd.service`

# Applying Updates to Change Guardian Components

You can use Agent Manager to upload the agent packages or the Policy Editor patch. These packages deploy bug fixes and improvements made to Change Guardian Agent for Windows, Change Guardian Agent for UNIX, or Policy Editor.

**To apply the patch**:

1. Download the patch from the Downloads website.
2. Log in to Agent Manager.
3. Click **All Assets** > **Manage Installation** > **Upload Package**.

   This uploads the package to the Change Guardian forwarder.
4. To upgrade agents or download Policy Editor, log in to Agent Manager on the machine running the agent or Policy Editor.
5. (Conditional) To upgrade Policy Editor, click All Assets > Manage Installation > Download Package, and then begin upgrade.

   The process of upgrading and installing the Policy Editor is the same. For more information, see Installing Policy Editor.

   **IMPORTANT:** After upgrading the Policy Editor, ensure that you update the policies and reassign them to the agents or create new policies.
6. (Conditional) To upgrade agents, click **Manage Installation** > **Upgrade Agents**.

# 5 Post Install Forwarder Configurations

After installing the Change Guardian server, you must perform configurations such as event destination configuration, adding application licenses, and enabling event data. This chapter provides information on the following topics:

- "Configuring Agents" on page 43
- "Applying License Keys" on page 44
- "Data Retention Policy" on page 44
- "Configuring Connectors" on page 45
- "Configuring Event Destinations" on page 48
- "Enabling Event Data to Cloud" on page 49

## Configuring Agents

Once you have installed Change Guardian Agents, you can configure or group them. You can configure the agents using the web console:

To access the web console, open the following URL:

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

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

- "Creating Custom Groups" on page 43

### Creating Custom Groups

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

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

**To add:**

1. Click **CONFIGURATION > Agents > Manage Custom Groups**.
2. Click the plus icon, and specify the **Group Name**.
3. Click the plus icon to specify one or more conditions.
4. Edit the condition to add the list of agents
   - Specify the FQDN to search agent names matching the FQDN

- Specify the complete operating system name and version such as “Microsoft Windows Server 2019 Standard Edition (build 17763), 64-bit”
- Use wildcard (Ex: 1.1.1.*) to search agents matching the IP address pattern

5. Click **SAVE**.

You can modify and delete custom groups.

After creating custom groups, assign policies and policy sets. To know more about assigning policies, see Assigning Policies and Policy Sets.

# Applying License Keys

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

To add or renew a license:

- Log in to the web console. Click **Configuration** > **Application Licenses**.
- Click **Import License Key**.
- Click the **Edit** icon. Browse and select the license file.
- Click **Validate**.
- When the license file validation is successful, click **Apply**.

# Data Retention Policy

By default, the existing data retention policies are set to a minimum of 90 days. Complete the following steps to change the minimum number of days to 1:

1. Login to the web console. Navigate to **Administration** > **Storage** > **Events**.
2. Under **Data Retention**, you will see 5 default policies created. Click **Edit**.
3. Change the **Keep at least** option from 90 days to 1 day.
4. Repeat the step for all the default policies.

## Creating Data Retention Policy

A retention policy is created to segregate the event into multiple data partitions in order to enhance the server performance. The policy contains a filter that is used to identify the events for which the retention policy applies and the minimum and maximum number of days these events should be kept in the system.

1. Login to Change Guardian web console.
2. Navigate to **Administration** page. Click **Storage** > **Events**.
3. Under **Data Retention**, click **Create** to create a new policy.
4. Specify the following:

   **Policy name:** Set a name for the policy.

   **Criteria:** Set the policy as per the below criteria:

```
(estzhour:[0 TO 3])
```

**Keep at least:** Minimum number of days to retain the policy. Set the minimum number of days to 1.

**Keep at most:** Maximum number of days to retain the policy.

5. Repeat step 4 until you create multiple policies for 24 hours.
   - `(estzhour:[4 TO 7])`
   - `(estzhour:[8 TO 11])`
   - `(estzhour:[12 TO 15])`
   - `(estzhour:[16 TO 19])`
   - `(estzhour:[20 TO 23])`
6. Restart server service by running the command:

   ```
   rcsentinel restart
   ```

# Configuring Connectors

HTTP Sync Connector is primarily used to receive event data from the Agent to the Forwarder. Once the HTTP Connector is configured using default configuration, create the event destination for the agent to start sending event data. For more information, see Creating Event Destinations.

Sentinel Link Integrator Configuration sends event data from the Forwarder to Cloud Layer. For more information, see Enabling Event Data to Cloud. The Sentinel Link Integrator is configured at the forwarder to send the event data. Before you send events from the integrator, ensure that S Link server is running on the receiver computer.

**NOTE**

- If you are configuring the settings in a cloud forwarder, ensure that you are able to access the DNS or the IP address.
- If the host name is reachable, you can configure multiple forwarders from a single machine.
- If you are configuring the connectors in a proxy environment, ensure to enable the proxy settings. For more information, see Enabling Proxy Settings.

This section provides the following information:

## Configuring Default HTTP Sync Connector and S Link Integrator at Forwarder

1. Navigate to `/opt/arcsight/connectors/changeguardian/opt/novell/sentinel/bin/` and run the following script:

   ```
   ./config_connectors.sh
   ```

2 To login for the first time, use the following default credentials under Change Guardian server details:

**Host name**: IP address

**Username**: admin

**Password**: password

**Server Port**: configured port. The default port is 8443.

3 You will see the following options:

**1. Default configuration**

**2. Custom configuration**

**3. Exit**

For default configuration choose option **1**.

4 Provide the following details:

DNS name of the regional server.

The HTTP Connector and S Link Integrator are created successfully.

**NOTE:** To modify or delete the default setting, choose the custom configuration option.

## Custom Configuration of HTTP Connector

Using the custom configuration option, you can create and delete the HTTP connector. Complete the following steps to create the Connector:

1 Navigate to `/opt/arcsight/connectors/changeguardian/opt/novell/sentinel/bin/` and run the following script:

```
./config_connectors.sh
```

2 To login for the first time, use the following default credentials under Change Guardian server details:

**Host name**: IP address

**Username**: admin

**Password**: password

**Server Port**: configured port. The default port is 8443.

3 You will see the following options:

**1. Default configuration**

**2. Custom configuration**

**3. Exit**

For custom configuration choose option **2**.

4 You will see the following options:

**1. HTTP connector**

**2. Slink integrator**

**3. Exit**

To configure HTTP Connector choose method **1**.

5 You will see the following options:

**1. View HTTP Connector**

**2. Create HTTP Connector**

**3. Delete HTTP Connector**

**4. Exit**

Enter **2** to Create HTTP Connector.

6 Specify the name of the connector and port details to configure.

7 HTTP Connector is created successfully. To delete the HTTP Connector, follow the above steps until 5, and select **3. Delete HTTP Connector**.

**NOTE:** By default, there is one HTTP Sync Connector available at port 7443. This port cannot be deleted using custom configuration.

## Custom Configuration of S Link Integrator

Using the custom configuration option, you can create, update, and delete the S Link Integrator. Complete the following steps to create the Integrator:

1 Navigate to `/opt/arcsight/connectors/changeguardian/opt/novell/sentinel/bin/` and run the following script:

```
./config_connectors.sh
```

2 To login for the first time, use the following default credentials under Change Guardian server details:

**Host name**: IP address

**Username**: admin

**Password**: password

**Server Port**: configured port. The default port is 8443.

3 You will see the following options:

**1. Default configuration**

**2. Custom configuration**

**3. Exit**

For custom configuration choose option **2**.

4 You will see the following options:

**1. HTTP connector**

**2. Slink integrator**

**3. Exit**

To configure Slink integrator choose method **2**.

5 You will see the following options:

**1. View slink integrator**

**2. Create slink integrator**

**3. Update slink integrator**

**4. Delete slink integrator**

**5. Exit**

To create S Link Integrator, select **2**.

6. Provide the following details:

   DNS name of the regional server.

   The S Link Integrator is successfully created.

7. To update or delete the integrator, follow steps till 5 and select option **3** and **4** respectively.

# Configuring Event Destinations

An event destination is assigned to policies based on which, the agent will send or distribute the events data to respective destination.

When you create a policy, it automatically uses the default event destination. If you want to send event data to another destination, add an event destination to the policy or policy set. You can use the new event destination along with the default event destination or replace it. The updated event destination takes effect when the agent receives the updated policy information at the next heartbeat.

Following sections provide information about creating event destinations.

- "Creating Event Destinations" on page 48

## Creating Event Destinations

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

**To create an event destination:**

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

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

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

7 Click **OK**.

# Enabling Event Data to Cloud

Change Guardian collects events from various assets based on pre-configured Change Guardian policies. Events are collected by Change Guardian agents and are received by the Change Guardian server and displayed in the Events dashboard.

This section provides the following information:

- "Configuring Event Routing Rules" on page 49

## Configuring Event Routing Rules

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

Following sections provide information about configuring event routing rules.

- "Creating Event Routing Rules" on page 49
- "Ordering Event Routing Rules" on page 50
- "Activating or Deactivating an Event Routing Rule" on page 50

### Creating Event Routing Rules

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

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.

To create an event routing rule:

1. Login to the Change Guardian web console.
2. Navigate to **Administration** > **Routing** > **Event Routing Rules**.
3. Click **Create**.
4. Specify the **Name**. To set the **Criteria**, click the **+** icon and select the criteria based on your requirement.

   For example: **Change Guardian Events** with the criteria **pn:"NetIQ Change Guardian" AND (sev:[2 TO 5])** and click **Add**.
5. Under **Route to the following services**, choose **All**.
6. Under **Perform the following actions**, select **Send Events via Sentinel Link**. If the Sentinel link has been configured, you will see that the DNS name of the regional server and port 1290 appears.
7. Click **Save**. The event routing rule is created.

## Ordering Event Routing Rules

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

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

**To order event routing rules:**

1. From the web console, click **ADMINISTRATION > Routing** in the toolbar.

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

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

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

## Activating or Deactivating an Event Routing Rule

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

1. From the web console, click **ADMINISTRATION > Routing** in the toolbar.

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

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

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

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

# 6 Understanding Asset Monitoring

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

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

This section provides information about configuring the following assets:

- "Windows Monitoring" on page 51
- "Linux or UNIX Monitoring" on page 52

## Windows Monitoring

Change Guardian monitors the following in Windows:

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

This section provides the following information:

- "Implementation Checklist" on page 51
- "Prerequisites" on page 52
- "Categories of Change Guardian Policies for Windows" on page 52

### Implementation Checklist

Complete the following tasks to start monitoring Windows events:

| Task | See |
|---|---|
| Complete the prerequisites | "Prerequisites" on page 52 |
| Configure Change Guardian for monitoring | "Categories of Change Guardian Policies for Windows" on page 52<br>"Assigning Policies and Policy Sets" on page 63 |

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

### Prerequisites

Ensure that you have completed the following:

- Install Change Guardian Agent for Windows
- Install Policy Editor

### Categories of Change Guardian Policies for Windows

**File integrity:** Policies about changes to critical startup file

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

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

**Local users and groups:** Policies about the following:

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

**Processes:** Policies about executing undesirable processes

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

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

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

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

For information about creating policies, see “Creating Policies” on page 60.

After creating policies, you can assign them to assets. For information about assigning policies, see “Assigning Policies and Policy Sets” on page 63.

## Linux or UNIX Monitoring

Change Guardian monitors the following in Linux and UNIX environments:

- Configuration files
- Local and exported file systems

- File integrity
- Groups
- Mounts
- Processes and daemons
- CRON jobs
- Users

This section provides the following information:

- "Implementation Checklist" on page 53
- "Prerequisites" on page 53
- "Categories of Change Guardian Policies for UNIX" on page 57

## Implementation Checklist

Complete the following tasks to start monitoring Linux and UNIX events:

| Task | See |
|---|---|
| Complete the prerequisites | "Prerequisites" on page 53 |
| Configure Change Guardian for monitoring | "Categories of Change Guardian Policies for UNIX" on page 57<br>"Assigning Policies and Policy Sets" on page 63 |

## Prerequisites

Ensure that you have completed the following:

- Install Change Guardian Agent for UNIX
- Install Policy Editor
- Configure Auditing in UNIX or Linux

### Auditing in UNIX or Linux

You must enable the auditing system of your UNIX or LINUX operating systems to allow Change Guardian to start monitoring.

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

- "Configuring a Linux Auditing Subsystem" on page 54
- "Configuring AIX Audit Subsystem" on page 54

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

## Configuring a Linux Auditing Subsystem

For RHEL and SUSE platforms, configure the audit daemon in the `/etc/audit/auditd.conf` file.

**To configure:**

1 (Conditional) For RHEL, ensure that the `auditd` service is enabled:

```
chkconfig auditd on
```

2 (Conditional) For SUSE, perform the following steps:

**2a** Check if the audit process is running:

```
ps -ef | grep -i audit
```

**2b** If the audit process is running in disabled mode, enable the process:

`/sbin/auditd -s enable`.

**2c** Ensure that the PID in the command output matches the PID of the enabled process:

```
auditctl -e 1
```

**2d** To enable syscall auditing:

Comment out the line `-a task,never` from the below file:

`/etc/audit/rules.d/audit.rules`. Restart the audit service.

For agents that are running on Linux platforms, additional audit configuration is performed dynamically as Change Guardian policies are enabled and disabled.

## Configuring AIX Audit Subsystem

Auditing subsystem stores files in the `/etc/security/audit` folder. However, in AIX computers, streaming all events might consume too much memory or processor time and enable only the minimum required auditing.

You can enable AIX audit subsystem either in STREAM or BIN mode.

**To configure AIX audit subsystem:**

1 Ensure that the `/etc/security/audit/config` file includes the following lines:

```
start:

bin:
     trail = /audit/trail
     bin1 = /audit/bin1
     bin2 = /audit/bin2
     binsize = 10240
  cmds = /etc/security/audit/bincmds
stream:
  cmds = /etc/security/audit/streamcmds
classes:
     general =
USER_SU,PASSWORD_Change,FILE_Unlink,FILE_Link,FILE_Rename,FS_Chdir,FS_
Fchdir,FS_Chroot,PORT_Locked,PORT_Change,FS_Mkdir,FS_Rmdir,FILE_Symlin
k,USER_Exit,PROC_Create,PROC_Delete,FILE_Fchmod,FS_Rmdir,GROUP_User,GR
OUP_Adms,GROUP_Change,GROUP_Create,GROUP_Remove,USER_Remove,USER_Creat
e,USER_Chpass,USER_Change,FS_Mount,FS_Umount,FILE_Unlinkat,FILE_Symlin
```

```
kat
     Kernel =
PROC_Create,PROC_Delete,PROC_Execute,PROC_RealUID,PROC_AuditID,PROC_Re
alGID,PROC_Environ,PROC_SetSignal,PROC_Limits,PROC_SetPri,PROC_Setpri,
PROC_Privilege,PROC_Settimer,PROC_LPExecute,PROC_Adjtime,PROC_Kill
     files =
FILE_Open,FILE_Read,FILE_Write,FILE_Close,FILE_Link,FILE_Unlink,FILE_R
ename,FILE_Owner,FILE_Mode,FILE_Acl,FILE_Privilege,DEV_Create,FILE_Dup
fd,FILE_Chmod,FILE_Chown,FILE_Utimes,FILE_Truncate,FILE_Mknod,FILE_Sym
link,FILE_Unlinkat,FILE_Fchownat,FILE_Linkat,FILE_Fchown,FILE_Symlinka
t,FILE_Openxat,FILE_Mknodat,FILE_Renameat,FILE_Fchownat,FILE_Fchmod,FI
LE_Fchown,FILE_Fchmodat
     cron =
AT_JobAdd,AT_JobRemove,CRON_JobAdd,CRON_JobRemove,CRON_Start,CRON_Fini
sh
users:
     root = general,Kernel,files,cron
     default = general,Kernel,files,cron
role:
```

**2** (Conditional) To enable `STREAM` mode, perform the following steps:

**2a** Add the following to `/etc/security/audit/config` file:

```
start:

     binmode = off

     streammode = on
```

**2a1** Add the following line to the`/etc/security/audit/streamcmds` file:

```
/usr/sbin/auditstream | /usr/sbin/auditpr -t 0 -r -v -
helRtcrpPTh >> /audit/trail&
```

**3** (Conditional) To enable `BIN` mode, perform the following steps:

**3a** Disable stream mode and enable bin mode in the `/etc/security/audit/config` file

**3b** Add the following line to`/etc/security/audit/bincmds` file:

```
/usr/sbin/auditcat $bin | /usr/sbin/auditpr -t 0 -r -v -helRtcrpPTh
>> /audit/trail
```

**3c** Add the following line to`/etc/security/audit/streamcmds` file:

```
/usr/sbin/auditstream | /usr/sbin/auditpr -t 0 -r -v -helRtcrpPTh >>
/audit/trail&
```

**4** Ensure that the `/etc/security/audit/events` file contains the following:

- FS_Mount
- FILE_Unlinkat
- CRON_Finish
- FILE_Linkat
- CRON_JobRemove
- PROC_Kill

- PROC_Execute
- FILE_Unlink
- FILE_Rename
- FILE_Fchown
- FILE_Owner
- USER_Chpass
- FILE_Symlinkat
- USER_Change
- FILE_Symlink
- PROC_LPExecute
- FILE_Open
- FILE_Mknodat
- FILE_Dupfd
- FILE_Chmod
- FILE_Renameat
- USER_Create
- GROUP_Create
- FS_Chdir
- FS_Umount
- FILE_Chown
- FILE_Fchownat
- GROUP_Change
- PROC_Create
- USER_Remove
- FILE_Fchmod
- PROC_Adjtime
- CRON_JobAdd
- FILE_Utimes
- PROC_Delete
- FILE_Openxat
- GROUP_Remove
- FILE_Fchmodat
- FILE_Mode
- PROC_Settimer
- FILE_Mknod
- CRON_Start
- FILE_Link

5 Restart the audit subsystem.

6 Restart `detectd` service from the given location:

```
/usr/netiq/pssetup/./detectd.rc restart
```

## Categories of Change Guardian Policies for UNIX

**Configuration Files:** Policies about changing hostname resolution and process startup configuration

**CRON:** Policies to monitor accessing CRON job, and changing CROS task execution

**Exported File System:** Policies to monitor list of exported file system

**File Integrity:** Policies to monitor Change Guardian Agent for UNIX configuration and system message of the day

**File System:** Policies to monitor bash shell startup configuration

**Groups:** Policies to monitor inbuilt groups

**Mount:** Policies to monitor CD-ROM mounts

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

**Users:** Policies to monitor built-in users

For information about creating policies, see "Creating Policies" on page 60.

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

To enable browsing for UNIX data sources while creating a policy, ensure that the machine where you install the Policy Editor must have a Change Guardian Agent for Windows. If you do not install an agent on the machine running Policy Editor, you must manually enter the data source paths while creating a policy.

**To enter the data source paths:**

1. (Conditional) If your operating system is 64-bit, in the registry `\HKLM\SOFTWARE\Wow6432Node\NetIQ\ChangeGuardianAgent\repositoryEnabled` set the `repositoryEnabled` flag to 1.
2. Restart the Change Guardian Agent for Windows.

# 7 Change Guardian Policies

Policies allow you to define how Change Guardian monitors assets in your environment. A policy includes one or more criteria to define a specific change event you want to monitor in your enterprise. Change Guardian collects events based on the Change Guardian policies. This chapter provides an overview about policies, information about how to create policies and policy sets, assign event designations to a policy, and so on.

## Understanding Policies and Policy Sets

Policies allow you to identify the asset you are monitoring, and then add any combination of the following criteria:

- Add filters to narrow the monitoring target and results
- Define managed users for the activity
- Assign event contexts to categorize policies
- Specify a custom severity that matches the policy

Each Change Guardian application includes several policy types.

You must apply a policy to an agent that is collecting events from the asset. You can combine multiple policies from one or more agents to organize and manage monitoring the agents. You can include a policy in multiple policy sets.

### Understanding Policy Attributes

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

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

**NOTE:** Change Guardian automatically calculates Event Severity for Change Guardian Agent for UNIX events, including events generated by policies configured with a custom severity.

Examples of severity are as follows:

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

**Managed User:** Change Guardian allows managed users to make specific changes to assets. When managed users make changes, the generated events appear as managed change events. When creating or editing a policy, use the **Managed Events** to specify the managed users for the policy.

If you specified a user group as a managed user, and the group membership changes, Change Guardian synchronizes associated policies with the new group members.

**Event Context:** Use the Event Context section to categorize the policy and specify its purpose. Generated events include the event contexts. You can create new event contexts with user-defined values. You can select one or more of the following default event contexts:

- Risk Domain
- Risk
- Sensitivity
- Regulation/Policy
- Control/Classification
- Response Window

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

Configure LDAP server for every grouped resource. You can either add the Active Directory items manually or browse them while creating a policy. A policy cannot monitor the group members correctly if you only specify the grouped resource in a policy, but do not configure LDAP settings for the grouped resource.

# Creating Policies

You can create a policy by using one of the following methods:

- Create a fresh policy with no preconfigured settings
- Clone and customize a template

**NOTE:** When there are multiple forwarders, you can configure policies in one forwarder and replicate to the other forwarders using Export Import Tool. For more information, see Export Import Tool.

## Creating a Fresh Policy

You can create a fresh policy without preconfigured settings.

**To create a policy:**

1. Login to Policy Editor.
2. Select one of the applications, such as Windows.
3. Expand the list of policies and select the policy type you want to create. For example, select **Windows Policies > File System**.
4. On the Configuration Policy screen, make the appropriate changes.
5. (Conditional) If you want to enable the policy immediately, select **Enable this policy revision now**.

**NOTE:** For more information about enabling a policy, see "Enabling a Change Guardian Policy Revision" on page 62.

# Working with Policies

Change Guardian stores the policies in the Change Guardian policy repository.

After creating a policy, you can perform various activities such as clone a policy, assign the policy to an agent, and schedule policy monitoring. While working with policies, ensure that you follow the order specified below:

1. Submit a policy or make the policy available by cloning from a template
2. Enable the policy

This section provides the following information:

- "Cloning a Change Guardian Policy" on page 61
- "Creating Change Guardian Policy Sets" on page 62
- "Enabling a Change Guardian Policy Revision" on page 62
- "Scheduling Change Guardian Policy Monitoring" on page 62

## Cloning a Change Guardian Policy

Cloning a policy allows you to create a policy based on an existing policy and then make changes as required. By default, Change Guardian uses the latest revision of the selected policy when creating a clone. You can also select a specific policy revision.

### Cloning a Template

Policy templates provide examples of best configured policies that you can reuse. Applying a policy template from the platform template library clones the policy into your active policy area. Edit the criteria to specify the agent and files to be monitored.

**To clone from a template:**

1. In Policy Editor, under the desired application, select the template you want to apply.
2. Specify the required information, and click **Submit**.
3. (Conditional) If you want to enable the policy immediately, select **Enable this policy revision now**.

   **NOTE:** For more information about enabling a policy, see “Enabling a Change Guardian Policy Revision” on page 62.

## Creating Change Guardian Policy Sets

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

Use the Policy Set Manager to add, edit, or clone policy sets. To open Policy Set Manager, click **Change Guardian > Policy Set Manager**.

## Enabling a Change Guardian Policy Revision

When you change a policy, Change Guardian creates a new revision of that policy. Policy revisions allow you to keep and share work that is in progress. You can view all policy revisions and the version number of the currently enabled policy in Policy Editor. You can edit and enable a previous revision of a policy.

**To enable an older revision:**

1. Select the desired policy under the application name.
2. On the **History** tab, enable the required policy revision.
3. Assign the policy.

**NOTE:** If you update the revision of a policy that is already assigned, Change Guardian automatically updates all associated agents with the new revision of that policy.

## Scheduling Change Guardian Policy Monitoring

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

To create a monitoring schedule, in Policy Editor, click **Settings > Schedule Monitoring Time**. You can set the following schedule during which you want to suspend monitoring: Mondays from 3-5 p.m. and Tuesdays from 4-6 p.m.

# Assigning Policies and Policy Sets

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

Change Guardian provides the following types of asset groups:

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

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

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

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

**To assign:**

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

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

# Assigning Event Destinations

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

**To assign:**

1. Log in to the web console, click **CONFIGURATION > Policies > Assign Policies**
2. Select **Agents** or **Agent Groups** and click the edit icon under **Assign Unassign** option.
3. Select a policy set or policies to enable the **Event Destinations** option.
4. Once it is enabled, click **Event Destinations**.

5 Select a policy from the drop-down list and assign one or more event destinations.

6 Click **SAVE** and **APPLY**.

**NOTE:** Policies that are a part of a policy set are not shown in the *Policies* tab. They are available under *Policy Sets* and contain the properties of the set. If the set is assigned with additional destination, it reflects after an upgrade. If the policy is assigned with an additional destination before moving to the set, it is not retained post upgrade. Since the policy is no longer available under *Policies*, it cannot be assigned separately to any destination.

# Export Import Tool

The Export Import tool is used to export policies from a single source forwarder to one or more destination forwarders. The tool is bundled with the Policy Editor package.

**NOTE:** Before running the Export Import tool, ensure to create a policy in the source forwarder.

This section provides the following information:

- Prerequisites
- Exporting and Importing Policies

## Prerequisites

- Download Policy Editor. To install the Policy Editor, see Installing Policy Editor.
- Download and install .Net Core Runtime Framework 5.0 in the same machine where Policy Editor is installed. To install the framework, download the pe_prerequisite.zip file.
- Add the IP address of the installed Policy Editor in the below file location of the source and destination forwarders:

  `/opt/arcsight/connectors/changeguardian/var/opt/novell/sentinel/3rdparty/postgresql/data/pg_hba.conf` in the format:

  ```
  host  all  all  <PE windows box IP>/32 md5
  ```
- Update the Postgress configuration file path and properties in the source and destination forwarders to the following:

  `/opt/arcsight/connectors/changeguardian/var/opt/novell/sentinel/3rdparty/postgresql/data/postgresql.conf`.

  - `Listen_address = '*'`
  - `Port = 5432`
  - `standard_conforming_strings = on`
- **NOTE:** Instead of the Postgress Configuration Property under `listen_address`, you can also provide the IP address of the servers from where the policy needs to be imported.
- After adding the configuration, restart the db with the below commands:

```
rcsentinel force_stopdb
rcsentinel startdb
```

## Exporting and Importing Policies

To export and import policies from source forwarder to different destination forwarders, perform the following procedure:

- Navigate to the location `<installedfolder>\NetIQ\ChangeGuardianPolicyEditor\ExportImportTool`.
- Open the command prompt and perform the following steps:
  - If there is a single source forwarder and a single destination forwarder, run the below command:

    ```
    ExportImportTool.exe Connect --sh <Source Forwarder IP Address> --su
    dbauser --dh <Destination Forwarder IP Address>  --du dbauser.
    ```
  - If there is a single source forwarder and multiple destination forwarders, run the below command:

    ```
    ExportImportTool.exe Connect --sh <Source Forwarder IP Address> --su
    dbauser --dh <Destination Forwarder 1 IP Address>#<Destination
    Forwarder 2 IP Address>  --du dbauser.
    ```
- Enter the source forwarder and destination forwarder passwords.

**NOTE:** When you provide multiple destinations to a single source forwarder, ensure to set the same password to all destination forwarders.

# 8 Advanced Configurations

This section provides information about enabling proxy settings, reconfiguring agent, configurations using server prompt, and adding email servers:

- "Enabling Proxy Settings" on page 67
- "Reconfiguring Agent" on page 68
- "Configurations Using the Server Command Prompt" on page 68
- "Configuring Event Routing to Email Servers" on page 74

## Enabling Proxy Settings

Proxy servers act as intermediaries between client applications and other servers. In an enterprise setting, proxy servers provide control over the content consumed by the users across network boundaries.

**NOTE:** Ensure that you enable proxy settings in all the forwarders that require communication through proxy.

**NOTE:** Ensure that the proxy server allows port 1290 to communicate to regional servers configured in AWS.

To enable proxy settings:

1. Add the following properties to `/opt/arcsight/connectors/changeguardian/etc/opt/novell/sentinel/config/server-custom.conf` file

   - `Dhttps.proxyHost=<proxy server IP/Hostname>`
   - `Dhttps.proxyPort=<proxy port no>`

   Post addition of these properties, the `server-custom.conf` file will look like the below example:

   ```
   # Custom Server Properties
   # Custom Java additional properties should start from 101
   wrapper.java.additional.101=-Dhttps.proxyHost=192.168.0.1
   wrapper.java.additional.102=-Dhttps.proxyPort=3128
   ```

   **NOTE:** If you are using an http proxy server, then use Dhttp instead of Dhttps while editing the file.

2. Restart Change Guardian service using the command:

   ```
   rcsentinel restart
   ```

# Reconfiguring Agent

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

**To reconfigure:**

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

## Verifying Windows Agent Reconfiguration

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

## Verifying UNIX Agent Reconfiguration

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

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

Where `service_name` can be `detectd` and `vigilent`

- `detectd`: Monitors tasks and retrieves data.
- `vigilent`: Sends events to the Change Guardian server.

# Configurations Using the Server Command Prompt

This section provides the following information:

## Configuring Memory Settings

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

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

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

**NOTE:** By default, in RHEL SHMMAX is a low value, so it is important to modify it when installing to this platform.

## Configuring Server Date and Time Synchronization

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

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

## Verifying Server Hostname

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

1. Verify the hostname configuration:

   ```
   cat /etc/HOSTNAME
   ```

2. Check the server hostname setting:

   ```
   hostname -f
   ```

3. Verify the DHCP configuration:

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

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

4. Resolve the hostname to the IP address:

   ```
   nslookup FULLY_QUALIFIED_HOSTNAME
   ```

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

   ```
   nslookup FULLY_QUALIFIED_CHANGEGUARDIANSERVER_HOSTNAME
   ```

# Configuring Email Servers

Complete the following steps to configure SMTP:

- "Configuring Email Server With Change Guardian" on page 70
- "Adding Email Servers" on page 70

You can also configure email servers by using Policy Editor.

## Configuring Email Server With Change Guardian

**To configure:**

1. Export the certificate from the respective SMTP server site.
2. To import the certificate, run the following command:

```
/opt/arcsight/connectors/changeguardian/opt/novell/sentinel/jdk/jre/
bin/keytool -import -alias <Alias_Name> -keystore opt/arcsight/
connectors/changeguardian/opt/novell/sentinel/jdk/jre/lib/security/
cacerts -file /root/<Certificate_Name>
```

**NOTE:** This key is imported only when you want to configure a secure connection.

3. Restart the Change Guardian server:

```
rcsentinel restart
```

## Adding Email Servers

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

1. Change directory:

```
cd /opt/arcsight/connectors/changeguardian/opt/netiq/cg/scripts
```

2. Set the email host settings:

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

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

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

# Configuring Email Server to Receive Email Alerts

To receive alerts on emails, complete the following steps:

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

# Configuring Security Settings

This section provides the following information:

- "Using CA Signed Certificates" on page 71
- "Applying Updates for Security Vulnerabilities in Embedded Third-Party Products" on page 74

## Using CA Signed Certificates

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

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

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

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

### Web Server Certificate

The web server certificate is used for the following purposes:

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

### Javos and Agent Manager

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

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

### Configuring the TLS/ SSL Certificates for Web Server

Configuring the TLS/SSL certificates involves the following steps:

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

### Generating a Certificate Signing Request

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

1. Log in to the Change Guardian server as the novell user.
2. Create a certificate pair by using the following command:

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

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

### Getting the CSR Signed by the CA

1. Submit the CSRs to the CA for signature.
2. Obtain the signed certificate files from the CA.

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

### Importing the Digitally Signed Certificates into Change Guardian

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

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

To import the certificate files to the Change Guardian server:

1. Log in to the Change Guardian server as the novell user.
2. Back up the default self-signed certificate:

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

3. Copy the CA signed certificate to the Sentinel server:

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

4. Import the intermediate certificate:

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

5 Import the root certificate:

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

6 Import the signed certificate:

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

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

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

8 Restart Change Guardian:

```
rcsentinel restart
```

## Configuring the TLS/ SSL Certificates for Javos and Agent Manager

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

**To replace the self-signed certificates on the server:**

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

2 Switch user to `novell`.

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

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

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

6 Change the permission of the `certs` folder:

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

7 Rename the CA-signed certificate files as below:

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

8 Change the ownership of the CA-signed files:

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

9 Go to the `/opt/netiq/cgutils/bin` directory and run the following command:

```
./cg_cert_setup.sh
```

The required certificates are created in the `/opt/netiq/cgutils/certs/` directory.

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

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

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

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

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

**12** Confirm that the profile is enabled:

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

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

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

**14** Confirm that the profile is enabled:

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

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

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

**16** (Optional) To test if the certificates are replaced successfully, remotely deploy an agent using Agent Manager and generate an event.

### Applying Updates for Security Vulnerabilities in Embedded Third-Party Products

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

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

## Configuring Event Routing to Email Servers

Use Policy Editor to perform the following tasks:

- "Adding Email Servers to Change Guardian" on page 75
- "Creating and Configuring Notification Groups" on page 75

**Prerequisites:** Install Policy Editor. For more information on the installation of Policy Editor, see Installing Policy Editor.

## Adding Email Servers to Change Guardian

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

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

1. In the Policy Editor, select **Settings > Email Configuration**.
2. Under **Email Servers**, click **Add**.
3. Specify the name and description of the email server you want to add.
4. Specify values for the following fields:
   - **SMTP Host:** The fully qualified domain name of the email server computer.
   - **SMTP Port:** The remote SMTP port to use when communicating with the email server.
   - **Secure:** Specifies whether the connection to the SMTP computer must be a secure connection. If **Yes**, specify the protocol type. If you select **No**, the **SMTP Port** is set to **25** by default.
   - **From**: The return email address appearing on each email alert for this email server.
   - **Authentication Required:** Specifies whether the email server requires SMTP authentication to send email. If **Yes**, specify the following:
     - **User Name:** The user name to use when connecting to the SMTP server.
     - **Password:** The password corresponding to the specified SMTP user name.
   - **Protocol:** Specifies which protocol can be used for the email communication. You can select **SSL** or **STARTTLS**.

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

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

## Creating and Configuring Notification Groups

For each email server you add to Change Guardian, you must create one or more notification groups specific to that email server. A notification group specifies one or more recipients of the email alerts and contains change event information. When you assign email alerts to events (using the **ADMINISTRATION** tab in the web console), you can choose from the notification groups available for that email server.

**To create and configure a notification group:**

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

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

# 9 Monitoring Events and Agent Health

Change Guardian provides Windows and UNIX based software that collects event data from the assets and forwards them to the Change Guardian server. You can view the health status of the agents and troubleshoot whether an agent is not running or not sending events to the server. This section provides information on viewing events, exporting events, viewing the agent health status and scheduling agent health reports.

- "Events" on page 77
- "Agent Health" on page 79

## Events

A Change Guardian event contains information such as the name of the event, who generated the event and where, the change that triggered the event, the before and after values, and the Change Guardian policy that triggered the event. You can generate an Event Summary report to view the event details.

### Viewing Events

You can view events from the **Events** dashboard in the Change Guardian web console. The dashboard provides a high-level overview of the events collected by the Change Guardian server. You can use this dashboard to monitor the changes happening in the environment, analyze the event, and take preventive steps to protect your organization from malicious attempts.

The dashboard provides the following information:

- Number of events generated for each asset or application
- Number of events based on the severity
- Option to filter events:
  - By managed or unmanaged events. An event is categorized as a managed event if it is triggered by an authorized user. Any other user who triggers that event is considered unmanaged.
  - By users who generated most events.
  - By assets from which most number of events are generated.
  - By event categories.
  - By the policy type.
  - By time range of events.

**NOTE:** Change Guardian policies are refreshed based on the Polling Interval set in Agent Manager. If you modify a policy, the Events Dashboard displays the associated event only after the polling interval has passed.

## Exporting Events Report

You can export events report to a CSV file. To export the events report:

- Login to the web console and click **Reports** > **Event Report** > **Events Summary**.
- Click the **Export to File** icon. The events report starts exporting.

**NOTE:** The forwarder event limit must be less than the number of events you selected and the maximum event limit is 200000.

## Scheduling Events Report

You can schedule the events report to be sent to the specified email ID once, daily, weekly, or monthly. To schedule the events report:

**NOTE:** To schedule events report, ensure that you have configured your email. To know more about email configuration, see Configuring Email Servers.

- Login to the web console and click **Administration**.
- Click **Reports and Searches** and select the **Change Guardian** drop-down.
- Click **Change Guardian Events** and select the **Run** icon.
- In the **Run the Report** dialog box, set details such as **Run** frequency, **Start Time**, **Name**, **Data Sources**, **Date Range**, and **E-mail to**. The other details are set by default.
- Click **Run**. The Events report has been scheduled.
- You can view the scheduled reports under **Change Guardian Events**.

## Generating Email Report in CSV

By default, Change Guardian generates reports in PDF format. You can also generate reports in CSV format by making additional configurations to the Change Guardian server.

To generate an email report in CSV format:

1. Login to Change Guardian server as a Novell user.
2. Change to the directory:

   `/opt/arcsight/connectors/changeguardian/etc/opt/novell/sentinel/config`
3. Run the following command:

   ```
   cd /opt/arcsight/connectors/changeguardia/etc/opt/novell/sentinel/
   config/
   ```
4. Open the `obj-component.JasperReportingComponent.properties`file for editing:

   ```
   vi obj-component.JasperReportingComponent.properties
   ```
5. Edit the following entry:

   ```
   reporting.csv.enable=true
   reporting.csv.email=true
   ```

6 Restart the Sentinel server with the command:

```
rcsentinel restart
```

The email report will contain both CSV and PDF outputs.

# Agent Health

The Agent Health dashboard displays the health status of Change Guardian agents, which are associated with a stand-alone Change Guardian server. Using the dashboard, you can troubleshoot if an agent is down or does not send events to the server.

The heartbeat of Change Guardian Agent for Windows (Polling Interval) and Change Guardian Agent for UNIX (Heartbeat) determines the frequency at which agents send a heartbeat to the Change Guardian server.

Based on the heartbeat of agents, the status of agents is categorized as below:

- **Offline**: Agents that have missed a heartbeat goes to the offline state until the next heartbeat.
- **Warning**: Agents are in the warning state when they have a heartbeat but are not able to send events to the Change Guardian server.

  Click on the agent to view the diagnosis information.
- **Online**: Agents have a heartbeat and are sending events to the server.

## Scheduling Agent Health Report

You can schedule an agent health report and add a list of email IDs of users to notify when agents go offline. You can also schedule daily updates on the health of agents.

**NOTE:** To schedule agent health report, ensure that you have configured your email. To know more about email configuration, see Configuring Email Servers.

To schedule agent health report:

- From the **Dashboards** page, click **Agent Health**.
- Click **Notifications**. It takes you to the **Configuration** tab.
- Under **Health Notification**, select the **Notify when agents go offline** check box .
- Click the **Edit** icon and select one or more agents.
- Specify one or more email IDs and press **Enter**. The agent health report of the selected agents will be sent to the specified email ID.
- You can also schedule daily health status of all agents by selecting the **Schedule daily health status** check box.

# 10 Backing Up and Restoring Data

The Change Guardian backup and restore utility is a script that performs a backup of Change Guardian data and also allows you restore the data at any time on the Change Guardian server. This section provides the following information:

- "Running the Backup and Restore Utility Script" on page 81

## Running the Backup and Restore Utility Script

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

**Prerequisites:**

- Ensure that the time and timezone is same on both the source machine from where the backup is taken and the destination machine where the restoration of data will happen.
- Ensure that the IP address of both the source and destination machines are the same.

**To backup and restore:**

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

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

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

| 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 -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 restore -f /var/opt/novell/sentinel/data/<*my_full_backup*>.tar.gz | Restores the data from the specified filename.<br>**NOTE:** To successfully restore the data from backup, ensure that the backup file ownership is set to user `novell` and group `novell`. |

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

**NOTE:** When you perform a full system backup or configuration data backup using the parameter `-c`, restore the data on the same version of Change Guardian with the same type of data storage using which the data was backed up. Restoring data between different Change Guardian server versions might cause data incompatibility due to changes between the product versions.

# 11 Troubleshooting

This section contains some of the issues that might occur during installing or using Change Guardian, along with the actions to work around the issues.

## Issues in Change Guardian Forwarder

### Javos.log Displays SQL Error After Upgrading to Patch 2

**Issue**: When you upgrade to Change Guardian 6.2.1 Patch 2, the Javos log displays consistent SQL error with no functionality impacted. (`Defect 790018`)

**Workaround**: None.

### Unable to start nq_javos process after switching from legacy profile profile_iqc to profile_javos

**Issue**: When you switch from legacy profile (`profile_iqc`) to secure profile (`profile_javos`), Javos service does not start.

**Workaround**: Check the `/opt/netiq/cg/javos/javos.out` file for any errors. If you see any errors related to `/opt/netiq/cg/javos/javos.yml` file content missing, please check if the following lines are present in `/opt/netiq/cg/javos/javos.yml` file. If not, add the highlighted lines to the file. After updating the `/opt/netiq/cg/javos/javos.yml` file, restart the Javos service with the command: `/etc/init.d/nq_javos restart`.

**cacheUpdateInterval: 60.** Recommended value is 60, minimum value is 30.

Appenders:

**type: file**

currentLogFilename: `log/javos.log`

threshold: ALL

archive: true

archivedLogFilenamePattern: `log/javos-%i.log`

archivedFileCount: 5

maxFileSize: 2MB

**timeZone: system**

logFormat: `"%-5level [%date] [%t] %logger: %msg%n%rEx"`

## Windows Policy Assignment Fails Due to IP Address Change in the Server

**Issue**: When the host name or IP address of the Change Guardian server is changed, the existing agents and CAM fail to communicate and the policy assignment too fails.

**Workaround**: Update the Event Destination with the new host name or IP address, For more information, see Change of IP and Host Name of the Change Guardian Server.

## Firewall Status Shows 'Stopped' in Change Guardian Appliance Environments

**Issue**: The status of the `SuSEfirewall2` shows as "stopped" in the Change Guardian Appliance environments.

**Workaround**: Start the firewall and save the firewall configuration by using the command `#rcSuSEfirewall2 start` and `#chkconfig SuSEfirewall2_init on`.

## Configuring Change Guardian Appliance to Boot Normally

**Issue**: Rebooting the Change Guardian Appliance in Hyper-V causes it to go into emergency mode. This issue occurs because the operating system modifies the disk UUID during installation.

**Workaround**: Install Change Guardian 5.1 appliance in Hyper-V and then upgrade to Change Guardian 6.0 appliance to resolve this issue. Alternately, you can update the UUID.

**To update the UUID:**

1. (Conditional) If the Change Guardian Appliance rebooted into emergency mode, login as `root`.
2. Run the command `ls -l /dev/disk/by-id/` and note the actual UUID of the disk.
3. Run the command `cat` for each of the following files to identify the disk UUID entries therein:
    - **/etc/fstab**

- **/etc/default/grub**
- **/boot/grub2/grub.cfg**

4 Compare the actual disk UUID entries in `/dev/disk/by-id` for the SCSI partitions with those in each of the above files.

5 (Conditional) If the disk UUIDs in each of locations do not match the actual values, you must manually replace the incorrect values with actual values.

***Example 11-1*** *Modifying Disk UUIDs*

If the UUID entry in the `fstab, grub or grub.cfg` files is `14d53465420202020f21b50e22267274c823e145500a372b7`, but the UUID on disk is `360022480f21b50e22267145500a372b7`, there is a mismatch which you must manually correct.

Therefore, once the UUID entry is replaced with correct values in the `fstab, grub and grub.cfg` files respectively, the entries therein read as below:

- **/etc/fstab**

```
/dev/disk/by-id/scsi-360022480f21b50e22267145500a372b7-part1 / ext3
acl 1 1
```

- **/etc/default/grub**

```
 GRUB_CMDLINE_LINUX=" root=/dev/disk/by-id/scsi-
360022480f21b50e22267145500a372b7-part1 nomodeset quiet"
```

- **/boot/grub2/grub.cfg**

```
 linux /boot/vmlinuz-4.4.131-94.29-default root=UUID=ace9acb3-ac2b-
47f0-960d-5b7cd5b51b47  root=/dev/disk/by-id/scsi-
360022480f21b50e22267145500a372b7-part1 nomodeset quiet
```

6 (Conditional) To exit the emergency mode, reboot the virtual machine.

The SCSI disk partition UUIDs are detected correctly and the appliance boots normally.

## Manual Configuration Required to use Registry Browser

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

**Workaround:** Manually set the flag to `1`, when you use the Registry Browser, to avoid the error *Could not connect to Windows Data Source*. `(Bug 945225)`

## Cannot Connect to AD Hostname, Domain, or IP Address

**Issue**: The subject alternate name (SAN) in the AD certificate must exactly match the AD hostname, domain, or IP address to which you are trying to connect. If they do not match, the connection fails with an error message such as:

```
server0.0.log - CertificateException: No subject alternative DNS name
matching ip address/hostname/dns found.
```

**Workaround**: Regenerate the LDAP server certificate so that the SAN or the subject name of the certificate matches that of the LDAP server.

If you are unable to regenerate the LDAP server certificate, update `nq_ldap_expander` and `server.conf` files:

1. Open the `/etc/init.d/nq_ldap_expander` file.
2. Add the following text:

   `-Dcom.sun.jndi.ldap.object.disableEndpointIdentification=true`

   For example:

   ```
   RUNCMD="(cd ${PROCESS_BIN}; nohup  ${JAVA} -
   Dcom.sun.jndi.ldap.object.disableEndpointIdentification=true -jar ./
   ${DAEMON_FILE}.jar server ./${DAEMON_FILE}.yml > ${DAEMON_FILE}.out
   2>&1; rm ${PIDFILE}) &"
   ```
3. Open the `/etc/opt/novell/sentinel/config/server.conf` file.
4. Add the following text next to “`wrapper.java.additional.74=`”

   `-Dcom.sun.jndi.ldap.object.disableEndpointIdentification=true`

   For example:

   ```
   wrapper.java.additional.74=-
   Dcom.sun.jndi.ldap.object.disableEndpointIdentification=true
   ```
5. Go to `/opt/netiq/cg/scripts`.
6. Restart the services:

   `./cg_services.sh restart`

## Modifying the Certificate Validity Period

To modify the certificate validity period in Change Guardian server script and reconfigure agents:

1. Login to Change Guardian server as root and navigate to the following path:

   `/opt/netiq/cgutils/bin/`
2. Edit the file `createClientCerts.sh` to change value of `CertNumDays` from 36500 to 3650 days. Save the changes.
3. **To view the certificate validity period changes:**

   **3a** Updating the createClientCerts.sh file as in step 2 ensures that the validity is set to 3650 days for the fresh agent installations.

   **3b** For the existing agents, you must reconfigure the agents. Login to Change Guardian Web UI and use the steps in “Reconfiguring Agent” on page 68.

**4 (Conditional) To download the agent artifacts and certificates for fresh installations:**

**4a** For Change Guardian Agent for Windows follow the steps in “Installing Change Guardian Agent for Windows” on page 42.

**4b** For Change Guardian Agent for UNIX, follow the steps in “Installing Change Guardian Agent for UNIX” on page 52.

**5 (Conditional) Replacing the certificates for the existing agents:**

Download and extract the `ChangeGuardianAgentCertificates_<hostname>.zip` file.

**5a** To replace certificate in the Change Agent for UNIX, copy the extracted `vigilent-agent-pk.pem`, `vigilent-agent-cert.pem` and `javosca-bundle.pem` to `/usr/netiq/cmnagent/codecs/vosSSLCodec/iqlsaca/certs/`.

**5b** To replace certificate in the Change Guardian agent for Windows, copy the extracted `vigilent-agent-pk.pem`, `vigilent-agent-cert.pem` and `javosca-bundle.pem` to `C:\Program Files (x86)\NetIQ\ChangeGuardianAgent\codecs\vosSSLCodec\iqlsaca\certs`.

**5c** Restart the agent services.

# Issues on Change Guardian Agent for Windows

- “When You Update Change Guardian to the Latest Version and There are Older Version of Policies Existing, the Agents Show Warning State” on page 87
- “Error Appears in VigilEntAgent_8094.log (ERROR [Minifilter_Collector]) for Windows Machine” on page 87
- “Installing Change Guardian Agent for Windows Fails with SMB Protocol Mismatch” on page 88
- “Collecting Agent Logs” on page 88
- “Change the Agent Package Version” on page 88

## When You Update Change Guardian to the Latest Version and There are Older Version of Policies Existing, the Agents Show Warning State

**Issue**: When you are using the latest version of Change Guardian and there are old version of policies existing, the agents display warning state with the policies showing the errors `00002053` and `00002052`.

**Workaround**: Update the existing policies, revise the policy version and reassign to agents or create new policies.

## Error Appears in VigilEntAgent_8094.log (ERROR [Minifilter_Collector]) for Windows Machine

**Issue**: Windows Agent VigilEntAgent_8094.log shows the error `Minifilter_Collector`.

**Workaround**: Reconfigure the agent through Agent Manager to address these errors.

## Installing Change Guardian Agent for Windows Fails with SMB Protocol Mismatch

**Issue**: Change Guardian Agent for Windows installation fails displaying the following error message in failed task logs:

```
Protocol negotiation failed...
```

The error might occur due to the following reasons:

- SMB1 protocol is disabled on Change Guardian Agent for Windows.
- Change Guardian server is installed on a Linux version that does not support SMB Version 2 (such as SLES 11.x or RHEL 6.x that has kernel version 2.6.x or lower), but only supports SMB Version 1. (`Bug 1155405`)

**Workaround**: Upgrade the operating system, on which Change Guardian server is running, to a version that supports SMB Version 2.

Alternatively, you can manually install the latest version of Change Guardian Agent for Windows. For more information, see Installing Change Guardian Agent for Windows.

## Collecting Agent Logs

You can use Agent Manger to collect logs from Change Guardian Agent for Windows. For more information, see "Collecting Agent Logs" on page 90.

## Change the Agent Package Version

**Issue**: You have a requirement to roll back to an older version of the agent package, but Agent Manager does not allow you to change the agent package version. (`Bug 1155538`)

**Workaround**: You can enable a new package, and disable the previous package by using the following file: `/opt/netiq/ams/ams/repository/packageActiveStatus.new.example`.

# Issues on Change Guardian Agent for UNIX

- "Agent Not Listed After Installation" on page 89
- "Unable to Connect to Port" on page 89
- "Unable to Run the Services" on page 89
- "Policies Are Not Applied to the Agent" on page 89
- "Events are not Generated After Configuring Change Guardian Agent for UNIX" on page 90
- "Collecting Agent Logs" on page 90

## Agent Not Listed After Installation

**Issue**: After a successful installation of the UNIX Agent, the agent does not list under the Agent Health page.

**Workaround**: Reconfigure the agent through Agent Manager.

## Unable to Connect to Port

**Issue**: Change Guardian Agent for UNIX is not able to connect to port 8094.

**Workaround**: Check whether the port 8094 is running:

```
netstat -an | grep 8094
```

## Unable to Run the Services

**Issue**: Change Guardian Agent for UNIX services are not running.

**Workaround**:

**1** Check if the `detectd` and `auditd` services are running:

```
ps -ef | grep "detect"
ps -ef | grep "auditd"
```

**2** (Conditional) If the services are not running, restart the following services:

**2a** Restart `auditd` service:

```
service auditd restart
```

**2b** Go to the `- /usr/netiq/pssetup` directory and run the following command:

```
./detectd.rc restart
```

**2c** Restart `vigilentagent` service:

```
./vigilentagent.rc restart
```

## Policies Are Not Applied to the Agent

**Issue**: The policies are not applied to the Change Guardian Agent for UNIX after it is assigned using Policy Editor.

**Workaround**: To verify whether the policies are applied to the agent after they are assigned in Policy Editor, check if the `<rule>.xml` file is created in the computer in the following directory:

```
/usr/netiq/vsau/etc/detectd.d/groups/<platformauditobject>/rules/
```

## Events are not Generated After Configuring Change Guardian Agent for UNIX

**Issue**: Change Guardian Agent for UNIX fails to send events to the Change Guardian Server if the locale setting is incorrect. `(Bug 1102111)`

**Workaround**: Ensure that the following is set:

1. The path is set at the operating system: `SET_PERL_LIBPATH=1; ./etc/vsaunix.cfg`
2. The locale variables are added to the `/etc/profile` file:
   - `export LC_CTYPE=en_US.UTF-8`
   - `export LC_ALL=en_US.UTF-8`

## Collecting Agent Logs

You can use Agent Manger to collect logs from Change Guardian Agent for UNIX. You must install the agent using Agent Manager to be able to collect the agent logs.

You cannot set debug levels to agent log collection. The logs are collected based on whatever debug level is set in the agent.

**To collect agent logs:**

1. In Agent Manager, select the agent under **All Assets**.
2. Click **Manage Installation > Collect Agent Logs > Start Log Collection**.
3. In the **Completed Tasks** tab, click **Download Agent Logs**.

**NOTE:** You can download a log only once. For an agent, you can download the log that you collected last. The previously collected logs are overwritten every time you click **Collect Agent Logs** for that agent.

# Troubleshooting Notes

## Change Guardian Forwarder Issues

- Server unresponsive
- Authentication failures
- Event/ Alert migration failures
- Database migration failures
- LDAP Authentication issues, etc.

## How to Troubleshoot?

1. Check status of ports:
   - Webserver/ 8443
   - PostgreSQL/5432
2. Check Firewall status
3. Check whether the product RPMS are installed and upgraded successfully
4. Logs to be collected:
   - `/opt/arcsight/connectors/changeguardian/var/opt/novell/sentinel/log`

# Change Guardian Agent Issues

- Agent deployment/ upgrade through AMS failures
- Heartbeat, Agent health issues
- Policy Assignment and Event generation failures, etc.

## How to Troubleshoot?

1. Check status of ports in server
   - Agent Manager/8082
   - JAVOS/8094
   - LDAPExpander/8079
2. Check whether the install and upgrade is completed successfully
3. Logs to be collected:
   - In server machine:
     - AMS logs: `/opt/arcsight/connectors/changeguardian/var/opt/netiq/ams/ams/log/ams.log ; /opt/arcsight/connectors/changeguardian/var/opt/netiq/ams/assets/log/assets.log`
     - JAVOS: `/opt/arcsight/connectors/changeguardian/var/opt/netiq/cg/javos/log/javos.log`
     - Certificate setup logs: `/opt/arcsight/connectors/changeguardian/var/opt/netiq/cgutils/certs/cert-setup.log`
   - In Agent machines:
     - Agent logs: `C:\ProgramData\NetIQ\ChangeGuardianAgent\`
     - CAM logs: `C:\ProgramData\NetIQ\ClientAgentManager\`

# A Appendices

This chapter provides information about the following:

- "Uninstalling Change Guardian" on page 93

## Uninstalling Change Guardian

- "Checklist to Uninstall" on page 93
- "Uninstalling Change Guardian Agent for Windows" on page 94
- "Uninstalling Change Guardian Agent for UNIX" on page 94
- "Uninstalling Policy Editor" on page 95
- "Uninstalling Change Guardian" on page 95
- "Tasks After Uninstalling" on page 95

### Checklist to Uninstall

Use the following checklist to uninstall Change Guardian:

- Uninstall the following components before you uninstall Change Guardian:
  - Change Guardian Agent for Windows and Change Guardian Agent for UNIX using Agent Manager
  - Policy Editor
- Complete the tasks after uninstalling to verify that Change Guardian is uninstalled
- Uninstall agents before uninstalling Change Guardian and the components

| Task | See |
|---|---|
| Uninstall the components | "Uninstalling Change Guardian Agent for Windows" on page 94<br>"Uninstalling Change Guardian Agent for UNIX" on page 94<br>"Uninstalling Policy Editor" on page 95 |
| Uninstall Change Guardian | "Uninstalling Change Guardian" on page 95 |
| Perform the post-uninstall steps | "Tasks After Uninstalling" on page 95 |

# Uninstalling Change Guardian Agent for Windows

Ensure that you have removed assets using Agent Manager.

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

- "Uninstalling Remotely" on page 94
- "Uninstalling Manually" on page 94

## Uninstalling Remotely

1. Login to Change Guardian web console and navigate to **Agents**.
2. Select the assets from which you want to uninstall the agent.
3. Select **Manage Installation > Uninstall Agents**.
4. Click **Start Uninstall**.

## Uninstalling Manually

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

# Uninstalling Change Guardian Agent for UNIX

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

- "Uninstalling Remotely" on page 94
- "Uninstalling Manually" on page 94
- "Verifying Uninstall" on page 95

## Uninstalling Remotely

**To uninstall:**

1. Select the assets from which you want to uninstall the agent.
2. Select **Manage Installation > Uninstall Agents**.
3. Click **Start Uninstall**.

To verify that you have successfully uninstalled, navigate to respective asset. Ensure that the asset is not listed in the assets list.

## Uninstalling Manually

To uninstall the Agent locally, go to the installation directory, then run the following command as a root user:

```
./uninstall.sh
```

### Verifying Uninstall

Verify that you have successfully uninstalled by performing the following:

- Check if all the components are uninstalled

  Run vi command on `/etc/vsaunix.cfg` configuration file to check if the parameter `` `CGU_INSTALLED` `` is n
- Check that none of the services are running by navigating to the `/usr/sbin` folder
- Check if the folder structure is deleted
- Check if assets that are uninstalled are not listed in the assets list

## Uninstalling Policy Editor

**NOTE:** Before uninstalling Policy Editor, ensure `agent/agent groups` have been uninstalled.

**To uninstall:**

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

## Uninstalling Change Guardian

1. Log in to the Change Guardian server as root.
2. Access the following directory: `/opt/novell/sentinel/setup/`
3. Run the following command: `./uninstall–changeguardian`
4. When prompted to reconfirm that you want to proceed with the uninstall, press **y**.

## Tasks After Uninstalling

After you uninstall Change Guardian server:

- Reboot the computer to clear the cache files
- To ensure that the services are not running, run the following commands:

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

  **NOTE:** If the services are still running, reinstalling the Change Guardian server will fail with errors or exceptions. Rebooting the machine terminates any services that are running from the previous installation.
- Ensure that there are no files or system settings remaining from the previous installation