Change Guardian™ 6.0

Installation and Administration Guide

September 2020

Legal Notice

© Copyright 2020 Micro Focus or one of its affiliates.

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 9

1 Introduction 11

What is Change Guardian? . . . 11
How Change Guardian Works . . . 12
Change Guardian Architecture . . . 13

2 Planning the Installation 15

Implementation Checklist . . . 15
Understanding Licensing . . . 16
Evaluation Licenses . . . 16
Enterprise Licenses . . . 16
Application Licenses . . . 16
Understanding Ports Used . . . 17
Installation Options . . . 19
Traditional Installation . . . 20
Appliance Installation . . . 20
Security Considerations . . . 20
Traditional Installation . . . 20
Appliance Installation . . . 21

3 Installing Change Guardian 23

Installation Checklist . . . 23
Traditional Installation . . . 23
Prerequisites . . . 24
Performing an Interactive Installation . . . 25
Performing a Silent Installation . . . 28
Appliance Installation . . . 29
Registering the Appliance for Updates . . . 30
Installing Change Guardian Components . . . 31
Installing Policy Editor . . . 31
Installing Change Guardian Agent for Windows . . . 32
Installing Security Agent for UNIX . . . 34
Installing Change Guardian Event Collector Addon for Windows Agent . . . 37
Configuring Change Guardian . . . 39
Configuring Memory Settings . . . 39
Configuring Server Date and Time Synchronization . . . 39
Verifying Server Hostname . . . 39
Configuring FIPS 140-2 . . . 40
Changing Default Email Host Settings . . . 41
Verifying the Installation . . . 42

4 Getting Started 43

Understanding the Change Guardian Interfaces . . . 43
Change Guardian Web Console . . . 43
Policy Editor . . . 45
Adding a License Key. . . . 45
Adding the License Key for Server . . . 46
Adding License for Applications . . . 46
Configuring Security Settings . . . 47
Configuring TLS . . . 47
Configuring Certificates . . . 48
Applying Updates for Security Vulnerabilities in Embedded Third-Party Products . . . 50
Configuring LDAP . . . 50
Configuring LDAP for Authentication . . . 50
Configuring LDAP to Access Domain Controller . . . 52
Configuring Users and Roles. . . . 53
Overview . . . 53
Creating Roles . . . 54
Understanding Password Complexity. . . . 55
Creating Users . . . 56
Adding Assets . . . 56
Adding Assets . . . 56
Viewing Assets in Agent Manager . . . 57
Viewing Assets in Policy Editor . . . 57

5 Configuring Event Monitoring 59

Configuring Windows Active Directory Monitoring . . . 59
Implementation Checklist . . . 60
Prerequisites . . . 60
Configuring Active Directory . . . 60
Categories of Windows Active Directory Policies . . . 64
Configuring Group Policy Monitoring . . . 65
Implementation Checklist . . . 66
Prerequisites . . . 66
Configuring GPO . . . 66
Categories of GPO Policies . . . 68
Configuring Windows Monitoring . . . 69
Implementation Checklist . . . 69
Prerequisites . . . 69
Categories of Windows Policies . . . 69
Configuring Microsoft Azure Active Directory Monitoring . . . 70
Implementation Checklist . . . 71
Prerequisites . . . 72
Configuring Default Windows Registry Keys . . . 73
Configuring Change Guardian for Monitoring . . . 74
Categories of Azure AD Policies . . . 75
Troubleshooting . . . 76
Configuring AWS Identity and Access Management . . . 76
Implementation Checklist . . . 77
Prerequisites . . . 77
Configuring Change Guardian for Monitoring . . . 78
Categories of AWS IAM Policies . . . 78
Configuring Office 365 Monitoring . . . 79

Implementation Checklist . . . 79
Prerequisites . . . 80
Configuring Change Guardian for Monitoring . . . 80
Categories of Office 365 Policies . . . 80
Configuring Dell EMC Monitoring . . . 81
Implementation Checklist . . . 81
Prerequisites . . . 82
Configuring Change Guardian for Monitoring . . . 82
Categories of Dell EMC Policies . . . 83
Configuring Microsoft Exchange Monitoring . . . 83
Implementation Checklist . . . 84
Prerequisites . . . 84
Configuring Change Guardian for Monitoring . . . 85
Categories of Microsoft Exchange Policies . . . 85
Configuring NetApp Storage Monitoring . . . 86
. . . Implementation
Checklist . . . 86
Prerequisites . . . 86
Configuring the NetApp Native Auditing . . . 87
Configuring Change Guardian for Monitoring . . . 89
Categories of NetApp Policies . . . 91
Configuring Linux or UNIX Monitoring . . . 91
Implementation Checklist . . . 92
Prerequisites . . . 92
Categories of UNIX Policies . . . 92

6 Configuring Policies 95

Understanding Policies and Policy Sets . . . 95
Understanding Policy Attributes . . . 95
Creating Change Guardian Policies . . . 96
Creating a Fresh Policy . . . 96
Working with Policies . . . 97
Cloning a Change Guardian Policy . . . 97
Creating Change Guardian Policy Sets . . . 98
Assigning Policies and Policy Sets . . . 98
Enabling a Change Guardian Policy Revision . . . 98
Exporting and Importing Change Guardian Policies . . . 99
Assigning Event Destinations to Change Guardian Policies . . . 99
Scheduling Change Guardian Policy Monitoring . . . 99
Policy Reports . . . 100

7 Managing Events 101

Configuring Event Destinations . . . 101
Creating Event Destinations . . . 102
Assigning Event Destinations . . . 103
Configuring Event Routing Rules . . . 103
Creating Event Routing Rules . . . 103
Ordering Event Routing Rules . . . 104
Activating or Deactivating an Event Routing Rule . . . 105
Forwarding Events for Long-Term Retention . . . 105
Viewing Events . . . 105

8 Configuring Alerts 107

Understanding Alerts 107
Managing Alerts 107
Creating and Managing Alert Rules 108
Creating Alert Rules 108
Redeploying Alert Rules 110
Configuring Event Destinations to Generate Alerts 110
Creating and Managing Alerts Routing Rules 110
Creating an Alert Routing Rule 110
Ordering Alert Routing Rules 111
Analyzing Alerts 111
Configuring Alert Retention Policies 111

9 Configuring Email Notifications 113

Configuring Email Servers 113
Configure Email Servers to Change Guardian in FIPS Mode 113
Configure Email Servers to Change Guardian in Non-FIPS Mode 113
Adding Email Servers to Change Guardian 114
Creating and Configuring Notification Groups 114
Creating Rules to Send Emails 115

10 Configuring Data Federation 117

Overview 117
Configuring an Authorized Requestor for Data Federation 118
Enabling Data Federation 118
Using the Administrator Credentials to Add a Data Source Server 118
Using the Opt-in Password to Add a Data Source Server 119
FIPS in Data Federation 121
Importing Certificates into the FIPS Keystore Database 121
Viewing Search Activities 122
Modifying the Data Source Server Details 122
Troubleshooting 123
Permission Denied 123
Connection Down 123
Unable to View Raw Data 124
Problems While Adding Data Source 124
Some Events Are Only Visible from the Local System 124
Cannot Run Reports on the Data Source Servers 124
Different Users Get Different Results 124
Cannot Set the Administrator Role as the Search Proxy Role 124
Error Logs 124

11 Configuring Integrations with Other Software 127

Integration with SIEM Solutions 127
Integrating with Identity Management Solutions 127
Integrating with Active Directory 128
Integration with Identity Manager 129
Searching and Viewing Identity Information 129
Integration with Directory Resource Administrator 130

Setting Up Change Guardian 130
Setting Up DRA 130
Viewing DRA Events in Change Guardian 132
Viewing Change Guardian Reports in DRA 132
Issues Coexisting with Change Guardian 132

12 Backing Up and Restoring Data 133

Parameters for the Backup and Restore Utility Script 134
Running the Backup and Restore Utility Script 136
Restoring Data 138
Enabling Event Data for Restoration 138
Viewing Event Data Available for Restoration 139
Restoring Event Data 139
Configuring Retention Period 140

13 Upgrading Change Guardian 141

Upgrade Checklist 141
Prerequisite 142
Upgrading a Traditional Installation 142
Upgrading Change Guardian 142
Upgrading the Operating System 143
Upgrading the Appliance Installation 144
Running the Appliance Configuration Utility 144
Applying Updates 145
Upgrading Components 147
Upgrading Policy Editor 148
Upgrading Change Guardian Agent for Windows 148
Upgrading Security Agent for UNIX 148
Applying Updates to Change Guardian Components 148
Adding Application License after Upgrade 149
Post Upgrade Configuration 149
Updating the Keystore Password 149
Setting the Polling Interval in Agent Manager 150
Verifying the Upgrade 150
Troubleshooting 150
Deploying Alert Rules Fail 150
Change Guardian Configuration Fails after Appliance Installation Completes 151
Cleaning Up Data From PostgreSQL When Migration Fails 151

A Appendices 153

Appliance Upgrading Paths 153
Uninstalling Change Guardian 154
Uninstallation Checklist 154
Uninstalling Change Guardian Event Collector Addon for Windows Agent 154
Uninstalling Change Guardian Agent for Windows 155
Uninstalling Security Agent for UNIX 155
Uninstalling Policy Editor 156
Uninstalling Change Guardian 156
Post-Uninstallation Tasks 156
Configuring Auditing in UNIX or Linux 157

Configuring a UNIX Auditing Subsystem 157
Configuring a Linux Auditing Subsystem 160
Setting Up Assets for Monitoring. 161
Setting Up AWS 161
Setting Up Office 365. 163
Setting Up Dell EMC. 164
Setting Up Exchange 165
Collecting Agent Logs Using Agent Manager 168
Increasing Data Partition Size. 168
Migrating Agents to Agent Manager 169
Services of the Security Agent for UNIX 169
Troubleshooting 170
Configuring Change Guardian Appliance to Boot Normally 170
Administration Console is Blank on Internet Explorer After Logging in 171
Change Guardian Agent for Windows Installation Using Agent Manager Fails 171
Asset Monitoring Failure Reports are not Captured for All Event Types 172
Azure AD Monitoring Events are not Captured for All Event and Attribute Types 172
Manual Configuration Required to use Registry Browser 172
Restarting the Change Guarding server with FIPS Mode Enabled Logs an Exception 173
Change the Agent Package Version 173
Installing Change Guardian Agent for Windows Fails with SMB Protocol Mismatch 173
Change Guardian Web Console is Blank if the License Has Expired 173
Change Guardian is not Receiving Events from Dell EMC 174
Unable to Browse File Locations and AD Using Policy Editor File Browser 174
Troubleshooting Agents in Warning State 174
AD Certificate is not Signed by a Well Known CA 176
Cannot Connect to AD Hostname, Domain, or IP Address 177
Security Agent for UNIX. 177

About this Book and the Library

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

Intended Audience

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

Additional Documentation

The Change Guardian documentation library includes the following resources:

User Guide

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

Release Notes

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

1 Introduction

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

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 11
- "How Change Guardian Works" on page 12

What is Change Guardian?

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

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

Change Guardian provides the following protection measures:

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

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

- Centrally recording and auditing changes

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

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

How Change Guardian Works

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, risk value of an event, 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 softwares for further analysis, and for long term retention. You can forward events to another Change Guardian server, Sentinel server, or Splunk Enterprise Security.

Adam Mandari is the administrator and he would like to monitor who changes critical Human Resource files in his enterprise. To allow Change Guardian to monitor this event, Adam creates a Change Guardian policy for Windows with the following definition:

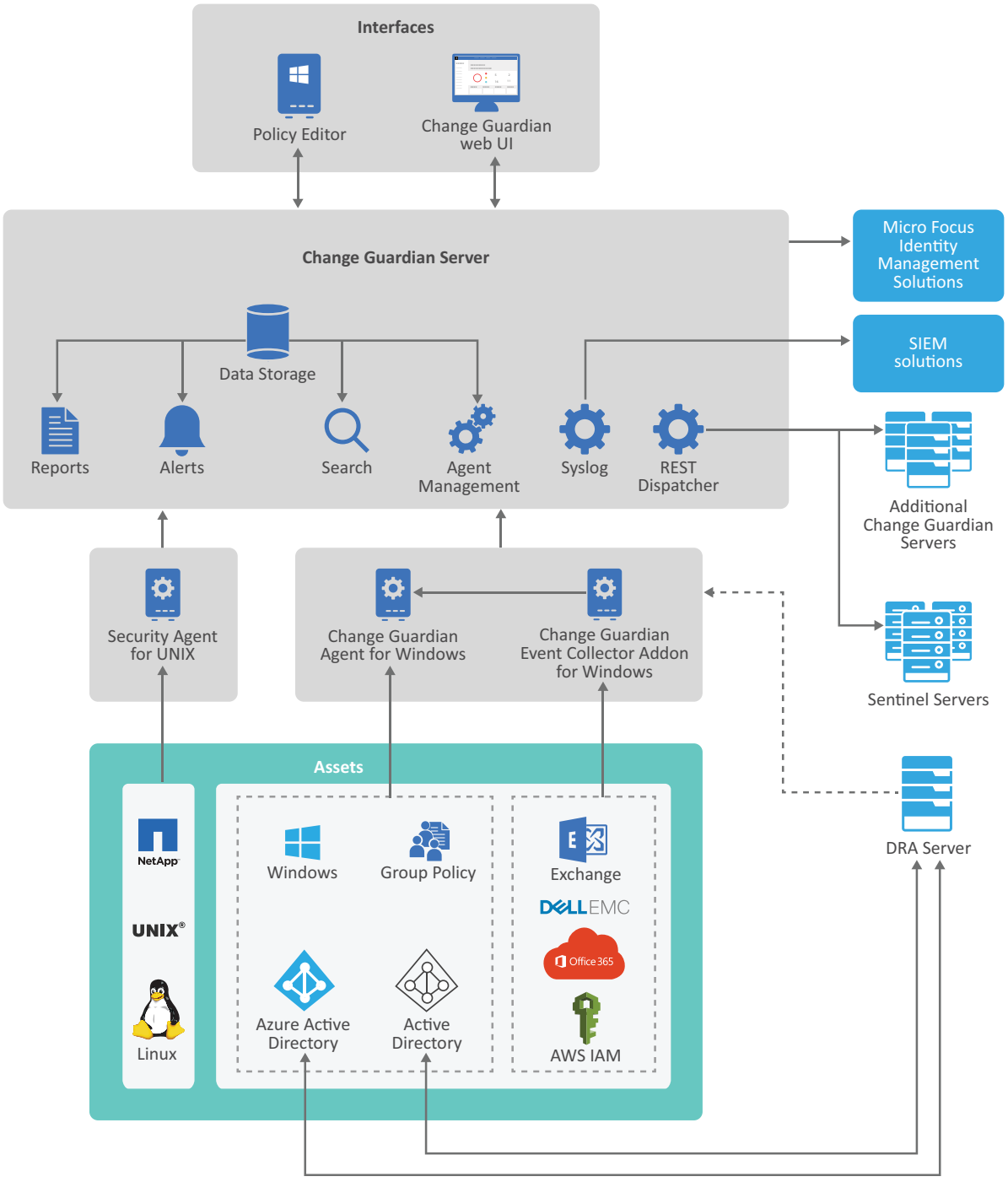
```
Monitors changes to contents in files in c:\payroll whose patterns match *
include only file content difference events
```

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. Adam configures an alert that notifies him whenever "File integrity was changed" event is generated. He uses the following interfaces to view the event and take necessary action:

- Change Guardian Dashboards: Allows you to view all events and manage alerts created using Change Guardian.
- Administration Console: Allows you to view and interact with data collected by Change Guardian.

Change Guardian Architecture

The following diagram illustrates how Change Guardian works:



Components in the Diagram	Description
Assets	Endpoints from where Change Guardian agents collect events.

Components in the Diagram	Description
Change Guardian Agents	Windows or UNIX based software that collects event data from the assets and forwards them to the Change Guardian server.
Change Guardian Event Collector Addon for Windows Agent	Collects event data in Common Event Format (CEF) from Dell EMC, Microsoft Exchange, AWS Identity and Access Management and Office 365. The Change Guardian Agent for Windows reads the event details in CEF.
Change Guardian Server	A Linux-based computer that receives and stores the event data. The server also stores the policies that you create. The server provides the capabilities of searching events and creating alerts and reports.
Agent Management	A central location where you can manage agents. Agent Manager allows you to deploy and manage your agents directly on the agent host machine, or remotely install agents.
Policy Editor	A Windows-based console where you create as well as deploy policies and alerts for asset monitoring.
Change Guardian Web UI	Interfaces to dashboards and management consoles where you can view events, view and triage alerts, create event and alert routing rule, manage users, and so on.

2 Planning the Installation

This section provides information about planning Change Guardian installation.

- "Implementation Checklist" on page 15
- "Understanding Licensing" on page 16
- "Understanding Ports Used" on page 17
- "Installation Options" on page 19
- "Security Considerations" on page 20

Implementation Checklist

Use the following checklist before you begin installing Change Guardian:

	Task	See
❑	Review product architecture information to learn about the software and components that you need to install and configure	Understanding How Change Guardian works
❑	Ensure that you have the necessary license keys	Understanding Licensing
❑	Review the hardware and software requirements, and the supported applications	Change Guardian System Requirements
❑	Determine whether you want to perform a traditional or an appliance installation of the Change Guardian server	Understanding the Installation Options
❑	Install the Change Guardian server	Installing the Change Guardian server
❑	Install the Change Guardian components	Installing Change Guardian Components
❑	Access the Change Guardian interfaces	Understanding the Change Guardian Interfaces
❑	Configure Policies	Configuring Policies
❑	Manage Events	Managing Events
❑	Configure Alerts	Configuring Alerts

Understanding Licensing

This section provides information about the following:

- "Evaluation Licenses" on page 16
- "Enterprise Licenses" on page 16
- "Application Licenses" on page 16

Evaluation Licenses

By default, a new installation of Change Guardian server includes evaluation licenses for Change Guardian and all applications. The default evaluation license allows you to use all the features of Change Guardian during for a specific evaluation period.

When you restore events from the server whose license expired to a server having a new license, the event dates are adjusted according to the new license.

NOTE: To prevent any interruption in functionality, you must add an enterprise license before the evaluation license expires. To purchase the enterprise license, contact Micro Focus Customer Care.

Enterprise Licenses

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

- HTML license key for the Change Guardian server
- XML license keys for each licensed applications (such as Active Directory or NetApp share)
- For appliance installation, you will also get an alphanumeric registration code to register your Change Guardian appliance to the appliance update channel

There might be additional license terms not enforced by the license key, therefore, read your license agreement carefully. To make changes to your licensing, contact Micro Focus Customer Care.

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

Application Licenses

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

Application Name	License Count
Microsoft Active Directory and Group Policy	Number of enabled active users in Active Directory
	Number of enabled active users in Group Policy
NetApp	Number of monitored NetApp instances
Microsoft Azure Active Directory	Number of enabled active users in Azure Active Directory
Microsoft Exchange Server	Number of active Exchange users
Dell EMC	Number of monitored Dell EMC instances
AWS (Identity)	Number of active AWS identities
Office 365 (Exchange Online)	Number of active users in Exchange Online

Understanding Ports Used

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

Component	Ports	Direction	Required /Optional	Description
Policy Editor Console	TCP 8443	Outbound	Required	Connects to the Change Guardian server for the following actions: ◆ Configuring email in Change Guardian or Sentinel. ◆ Updating policies to the Change Guardian server.
	TCP 2620	Outbound	Optional	Allows remote object browsing to UNIX-based monitored assets.
	TCP 389 or TCP 636	Outbound	Optional	Allows remote object browsing to Active Directory.
	TCP 8443	Inbound	Required	Allows the Change Guardian server to receive events from monitored assets. **NOTE:** This port might not be needed if you are sending events from monitored assets to an alternate destination.
Change Guardian Server	TCP 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.

Component	Ports	Direction	Required /Optional	Description
	TCP 1099 and 2000	Inbound	Required	Used together by monitoring tools to connect to Change Guardian server process using Java Management Extensions (JMX).
	TCP 5432	Inbound	Optional. By default, this port listens only on loopback interface.	Used for the PostgreSQL database.
	TCP 137, 138, 139, 445	Outbound	Optional	Used if secondary storage is configured to CIFS.
	TCP/UDP 111 and TCP/UDP 2049	Outbound	Optional	Used if secondary storage is configured to NFS.
	UDP 514 or TCP 1468	Outbound	Optional	Used when Change Guardian forwards events to the system receiving Syslog messages. If the port is UDP, it sends a packet to the receiver. If the port is TCP, it initiates a connection to the receiver.
	TCP 32000			Used for internal communication between the wrapper process and the server process.
	TCP 9200			Used for communication with alert indexing service using REST.
	TCP 9300			Used for communication with alert indexing service using its native protocol.
	TCP 443	Inbound	Optional	Forwarded to 8443 for HTTPS communication.
	TCP 61616	Inbound	Optional	Used for incoming connections from Correlation Engines.
	TCP 9443	Inbound	Required	Used by the Change Guardian Appliance Management Console.
JAVOS	TCP 8094	inbound	Required	Allows the JAVOS service to accept connections from agents that are retrieving their assigned monitoring policies.
	TCP 9094	Inbound (loopback)	Required	Allows the Change Guardian server to call JAVOS on this port to signal/reset the event destination cache.
	TCP 9095	Inbound (loopback)	Optional	Allows users to see runtime metrics and active threads.

Component	Ports	Direction	Required /Optional	Description
Active Directory Accounts/ LDAP Expander	TCP 8088	Inbound (loopback)	Required	Allows the Change Guardian server to retrieve information about Active Directory accounts.
	TCP 8089	Inbound (loopback)	Optional	Allows users to see runtime metrics and active threads.
Windows Monitoring Agents	TCP 8094	Outbound	Required	Allows the agent to connect to the Change Guardian server to retrieve assigned monitoring policies.
	TCP 8094	Inbound	Optional	Allows the Policy Editor to connect to the agent to browse objects on the monitored asset.
	TCP 8443	Outbound	Required	Allows the agent to connect to the Change Guardian server or Sentinel to send events.
UNIX Monitoring Agents	TCP 8094	Outbound	Required	Allows the agent to connect to the Change Guardian server to retrieve assigned monitoring policies.
	TCP 2620	Inbound	Optional	Allows the Policy Editor to connect to the agent to browse objects on the monitored asset.
	TCP 8443	Outbound	Required	Allows the agent to connect to the Change Guardian server or Sentinel to send events.
UNIX Agent Manager	TCP 2620	Outbound	Required	Allows the UNIX Agent Manager to connect to a UNIX agent to get status and diagnostic information.
	TCP 2222	Outbound	Required	Allows the UNIX Agent Manager client to connect with the UNIX Agent Manager server.
	TCP 22	Outbound	One of these is required.	Used by UNIX Agent Manager in SSH connections that required SSH+SFTP access to computers targeted for remote agent deployment.
	TCP 21/ 23	Outbound		Used by UNIX Agent Manager in Telnet/FTP connection that requires Telnet+FTP access to computers targeted for remote agent deployment.
Agent Manager	TCP 8082	Inbound	Required	Allows the agent to communicate with the Agent Manager.
	TCP 445	Outbound	Required	Allows the Agent Manager to deploy agents to Windows computers.
	TCP 22	Outbound	Required	Allows the Agent Manager to deploy agents to Windows computers.

Installation Options

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

Traditional Installation

This installation provides the following:

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

Appliance Installation

This installation provides the following:

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

Security Considerations

The following sections provide information about secured installations:

- "Traditional Installation" on page 20
- "Appliance Installation" on page 21

Traditional Installation

- 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.

Appliance Installation

The appliance has undergone the following hardening:

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

3 Installing Change Guardian

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

- “Installation Checklist” on page 23
- “Traditional Installation” on page 23
- “Appliance Installation” on page 29
- “Installing Change Guardian Components” on page 31
- “Configuring Change Guardian” on page 39
- “Verifying the Installation” on page 42

Installation Checklist

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

If you are upgrading from a previous version of Change Guardian, do not use this checklist. For information about upgrading, see Chapter 13, “Upgrading Change Guardian,” on page 141.

	Task	See
❑	Install Change Guardian.	“Traditional Installation” on page 23 “Appliance Installation” on page 29
❑	Install Change Guardian components.	“Installing Change Guardian Components” on page 31
❑	Configure Change Guardian.	“Configuring Change Guardian” on page 39
❑	(Conditional) If you change the IP address of the Change Guardian server, there is a break down of communication between the server and agent. This requires reconfiguration of the server to restore communication. Therefore, consider using static IP addresses in your Change Guardian deployment.	-

Traditional Installation

This section provides the following information:

- “Prerequisites” on page 24
- “Performing an Interactive Installation” on page 25
- “Performing a Silent Installation” on page 28

Prerequisites

Ensure that your system meets the following:

- Review the latest Change Guardian release notes to understand new features and known issues.
- FIPS mode is supported only for Change Guardian. Change Guardian is not supported if the operating system is in FIPS mode. Therefore, ensure that the operating system is not in FIPS mode.
- If there was a previous installation of Change Guardian, ensure that there are no files or system settings remaining from a previous installation.
- The operating system for the Change Guardian server must include at least the Base Server components of the SLES server or the RHEL server. Change Guardian requires the 64-bit versions of the following RPMs:
  - bash
  - bc
  - curl
  - expect
  - coreutils
  - gettext
  - glibc
  - grep
  - libgcc
  - libstdc
  - lsof
  - net-tools
  - openssl
  - python-libs
  - samba-client
  - samba-common-libs
  - samba-common-tools
  - samba-libs
  - sed
  - tcl
  - zlib
  - fontconfig
  - dejavu-fonts

Performing an Interactive Installation

This section provides information about standard and custom installation.

- "Standard Installation" on page 25
- "Custom Installation" on page 26

Standard Installation

Use the following steps to perform a standard installation:

To install the Change Guardian server:

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

   `tar zxvf cgserver-x.x.x-xx.x86_64.tgz`
3. Run the Change Guardian server installation program as `root` by typing the following command in the root of the extracted directory:

   `./install-changeguardian.sh`

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

   Or

   If you want to install Change Guardian on more than one system, you can record your installation options in a file. You can use this file for an unattended Change Guardian installation on other systems. To record your installation options, specify the following command: `./install-changeguardian.sh -r <response_filename>`
4. Specify the language as English, then press Enter. The end user license agreement is displayed in the selected language.
5. Press the space bar to read the license agreement. You must scroll through the entire agreement before you can accept it.
6. When prompted, select the standard configuration.

   The installation proceeds an evaluation license key included with the installer. You can replace the evaluation license with a license key you purchased.
7. Create an admin account password for global system administration.

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

   ---
8. Create a password for the `cgadmin` user.

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

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

   ---

9 If you want to email reports, configure the default email host using the following information:

- **SMTP Host:** The full name, including domain name, of the email server from which you want to send scheduled reports by email. Change Guardian server should be able to resolve the hostname.
- **SMTP Port:** The remote SMTP port, where the default number is 25. Use port 587 for a secure connection.
- **From:** The return email address.
- **SMTP User Name (Optional):** The user name to connect to the SMTP server.
- **SMTP Password (Optional):** The password that corresponds to the SMTP user name.
- **Secure Connection:** The connection mechanism for STARTTLS protocol.

NOTE: If you later decide to email reports and events, you must use the `configure.sh` script to update this configuration. For more information, see "Changing Default Email Host Settings" on page 41.

9a (Conditional) If the SMTP server certificate is self-signed or if not signed by a well-known CA, such as VeriSign, you have to import the certificate to the server trust-store. To import the self-signed certificate or CA certificate, complete the following steps:

9a1 Download the certificate to the server.

9a2 To store the certificate in `activemqkeystore`, run the following command on the server:

```
/opt/novell/sentinel/jdk/jre/bin/keytool -import -alias
<appropriate_alias> -keystore /etc/opt/novell/sentinel/config/
.activemqkeystore.jks -file <certificate_file_path> -storepass
password
```

9a3 Restart the server:

```
rcsentinel restart
```

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

Custom Installation

To install the Change Guardian server:

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

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

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

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

```
./install-changeguardian.sh --location=<custom_CG_directory_path>
```

NOTE: This custom path must have 0755 permissions.

Or

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

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

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

6 When prompted, select custom configuration, and provide the following information:

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

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

---

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

Assign dbauser account password: Account for PostgreSQL database maintenance

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

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

---

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

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

---

NOTE: Configuring FIPS using the custom configuration is currently not supported. For more information about configuring Change Guardian to run in FIPS mode, see "Configuring FIPS 140-2" on page 40

---

7 Create a password for the `cgadmin` user.

Use this account to log in to the Policy Editor. This account has the privilege to administer monitoring configuration.

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

---

8 Configure the default email host using the following information:

- **SMTP Host:** The full name, including domain name, of the email server from which you want to send scheduled reports by email. Change Guardian server should be able to resolve the hostname.
- **SMTP Port:** The remote SMTP port, where the default number is 25. Use port 587 for a secure connection.
- **From:** The return email address.
- **SMTP User Name (Optional):** The user name to connect to the SMTP server.
- **SMTP Password (Optional):** The password that corresponds to the SMTP user name.
- **Secure Connection:** The connection mechanism for STARTTLS protocol. Set the value to `true` if you want to configure SMTP server for STARTTLS.

NOTE: If you later decide to email reports and events, you must use the `configure.sh` script to update this configuration.

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

8a1 Download the certificate to the server.

8a2 To store the certificate in `activemqkeystore`, run the following command on the server:

```
/opt/novell/sentinel/jdk/jre/bin/keytool -import -alias
<appropriate_alias> -keystore /etc/opt/novell/sentinel/config/
.activemqkeystore.jks -file <certificate_file_path> -storepass
password
```

8a3 Restart the server by running the following command:

```
rcsentinel restart
```

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

Performing a Silent Installation

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

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

- Standard Installation
- Custom Installation

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

- ENABLE_FIPS_MODE
- NSS_DB_PASSWORD

To perform a silent installation:

1. Download the installation files from the Downloads website.
2. Log in as `root` to the server where you want to install Change Guardian.
3. Specify the following command to extract the install files from the tar file:

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

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

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

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

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

Appliance Installation

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

NOTE: Change Guardian 6.0 appliance installation is not supported on Hyper-V. Install Change Guardian 5.1 appliance in Hyper-V and then upgrade to Change Guardian 6.0 appliance.

Prerequisite: Ensure that the machine meets the hardware requirements. For hardware information, See System Requirements page.

To install:

1. Download the base appliance image to a local server from the Change Guardian downloads page.

   The OVF file name is `ChangeGuardian_SLES12SP5GM_6.0.0.0.x86_64-18.0.0.ovf.tar.gz`.

   The ISO file name is `ChangeGuardian_SLES12SP5GM_6.0.0.0.x86_64-18.0.0.preload.iso`.
2. (Conditional) If you are using VMware, use the OVF template to complete the following steps:
   - **2a** Extract the appliance image to your local server.

     If you are extracting to a Windows server, you need a program, such as WinRar:

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

     `tar -zxvf <filename>`
   - **2b** Log in to the vSphere client and deploy the OVF template. For more information, see the VMware documentation.
3. (Conditional) If you are using Microsoft Hyper-V or installing direct to hardware, use the ISO image to complete the following steps:
   - **3a** Burn the ISO file to a DVD or mount the image.

     NOTE: Change Guardian does not support mounting the ISO image from a network share.
   - **3b** Start or reboot your computer and check the BIOS configuration of your machine. The BIOS should allow you to start from the CD/DVD drive and change the order of the media.
   - **3c** (Conditional) If you have not mounted the image, boot the DVD.
4. Power on the appliance server.
5. Select the language and keyboard layout.
6. Read and accept the SUSE End User License Agreement.
7. Read and accept the Change Guardian End User License Agreement.

8 Set the Hardware Clock to UTC, specify the time zone of the VM, and then select **Change** to configure NTP date/time synchronization.

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

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

9 Configure the following:

   - Appliance OS root account password
   - global `admin` password

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

   - Create a password for the `cgadmin` user.
   - Deselect **Use IP Address for event routing** if the Change Guardian server can resolve the hostname.

10 (Optional) If you want to email reports, configure the default email host using the following information:

   - **SMTP Host:** The full name, including domain name, of the email server from which you want to send email alerts. Change Guardian server should be able to resolve the hostname.
   - **SMTP Port:** The remote SMTP port, where the default number is 25. Use port 587 for a secure connection.
   - **From:** The return email address.
   - **SMTP User Name (Optional):** The user name to connect to the SMTP server.
   - **SMTP Password (Optional):** The password that corresponds to the SMTP user name.

11 To ensure that the appliance does not go into emergency mode, change the SCSI disk partition UUID.

12 (Conditional) If javos service does not run after completing this step, reconfigure Change Guardian by using configure.sh.

Registering the Appliance for Updates

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

- "Register Using the Change Guardian Appliance Management Console" on page 30
- "Register Using Commands" on page 31

Register Using the Change Guardian Appliance Management Console

To register the appliance for updates:

1 Log in to the Change Guardian Appliance Management Console as `vaadmin` or `root`.

2 Click **Home > Online Update > Register Now**.

3 In the **Email** field, specify the email ID to which you want to receive updates.

4 In the **Activation Key** field, enter the registration code.

5 Click **Register**.

6 Verify whether updates are available.

Register Using Commands

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

1 Log in to the Change Guardian Appliance Console as `root`: `https://IP_Address_Change_Guardian_server:9443`.

2 Clean existing registrations for SLES (11 and 12) based clients:

```
suse_register -E
```

3 Register the server for SLES (11 and 12) based clients:

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

4 Verify whether updates are available.

Installing Change Guardian Components

To work with Change Guardian, you require a combination of the following components.

Policy Editor: Allows you to configure policies and assign policies to assets you want to monitor.

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

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

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

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

This section provides the following information:

- "Installing Policy Editor" on page 31
- "Installing Change Guardian Agent for Windows" on page 32
- "Installing Security Agent for UNIX" on page 34
- "Installing Change Guardian Event Collector Addon for Windows Agent" on page 37

Installing Policy Editor

To install Policy Editor:

1 In Agent Manger, click **Manage Installation > Download Package**.

2 Download the available version of Policy Editor.

3 Copy the `ChangeGuardianPolicyEditor.zip` file to the computer where you want to install Policy Editor and extract the files.

   The package includes `NetIQCGPolicyEditorInstaller.exe` and `NetIQCGPolicyEditorInstaller.config`. Both files must be in the same directory.

4 Install Policy Editor as an administrator.

Accessing Policy Editor

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.

NOTE: Always open Policy Editor account in the local administrators group.

Installing Change Guardian Agent for Windows

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

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

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

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

- "Remote Installation" on page 32
- "Manual Installation" on page 33
- "Reconfiguring the Agent" on page 34

Remote Installation

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

Prerequisite: Using Agent Manager, you must first add the assets where you want to install agents. You can either import assets from Active Directory or from a text file, or add assets manually. For more information, see "Adding Assets" on page 56.

To install Change Guardian Agent for Windows using Agent Manager:

1 In Agent Manager, select the asset where you want to deploy the agent. If you select multiple assets, they must use the same credentials.

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

3 For newly added assets, specify the `root` credentials and click **Next**.

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

4 Select the available version of the agent.

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

6 Click **Start Installation.**

Manual Installation

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

- "Downloading the Agent Certificates and Artifacts" on page 33
- "Installing the Agent" on page 33

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.

Reconfiguring the Agent

When you have to change an agent's configuration, for example enable or disable Event Collector Plugin, you must reconfigure the agent.

To configure:

1. In Agent Manger, do one of the following:
   - (Conditional) If you have not added assets previously, in Agent Manager, under **Asset Groups**, click **All Assets** and then click **Add Assets**.
   - (Conditional) If you have added assets previously, in Agent Manager, click **All Assets**, then **Manage Assets**, and then **Add**.
2. From the assets list, select the computers where you want to deploy the agent. If you select multiple computers, you must use the same credentials in all computers.
3. Log in as `root` to the computer that you want to connect and click **Next**.
4. Click **Manage Installation**, and then select **Reconfigure**.
5. Select the version and then select the default configuration, edit it or add a new configuration.

Installing Security Agent for UNIX

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

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

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

- "Interactive Installation" on page 34
- "Silent Installation" on page 35
- "Reconfiguration the Agent" on page 37

Interactive Installation

This section provides the following information:

- "Remote Installation" on page 34
- "Manual Installation" on page 35

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.

   If you select multiple machines, use the same credentials.
3. Click **Manage Installation > Install Agents**.
4. Provide the user name and password of the agent and click **Next** and start the installation.

NOTE: When you are installing Security 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 33.
2. Log in to an machine running the agent using an account with superuser privileges.
3. Click **All Assets > Manage Installation > Download**, and download the required package.

   Agent Manager downloads `SecurityAgentForUnix.zip` to your computer.
4. Extract `SecurityAgentForUnix.zip` to the computer where you want to install the Security 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 Security 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 Security Agent for UNIX.

Silent Installation

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

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

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

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

To install:

1. Download the installation files from the Downloads website.

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

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

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

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

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

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

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.
IQCONNECT_PORT	Specifies the port that the agent uses to listen for communications from UNIX Agent Manager. The default value is 2620.
IQ_STARTUP	Specify restart method for the agent process. For information about the options, see "Services of the Security Agent for UNIX" on page 169. 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 "Services of the Security Agent for UNIX" on page 169. 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.

Reconfiguration the Agent

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

To reconfigure:

1. In Agent Manger, do one of the following:
   - (Conditional) If you have not added assets previously, in Agent Manager, under **Asset Groups**, click **All Assets** and then click **Add Assets**.
   - (Conditional) If you have added assets previously, in Agent Manager, click **All Assets**, then **Manage Assets**, and then **Add**.
2. From the assets list, select the computers where you want to deploy the agent. If you select multiple computers, you must use the same credentials in all computers.
3. Log in as `root` to the computer that you want to connect and click **Next**.
4. Click **Manage Installation**, and then select **Reconfigure**.
5. Select the version and then select the default configuration, edit it or add a new configuration.

Installing Change Guardian Event Collector Addon for Windows Agent

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

Before installing the Change Guardian Event Collector Addon for Windows Agent, set up the required connectors:

- “Setting Up AWS” on page 161
- “Setting Up Office 365” on page 163
- “Setting Up Dell EMC” on page 164
- “Setting Up Exchange” on page 165

To install Change Guardian Event Collector Addon for Windows Agent:

1. In Agent Manager, click **Manage Installation > Download Package**.
2. Download Change Guardian Event Collector Addon for Windows Agent.

3 In the installer window, specify the local path in which you want to install Change Guardian Event Collector Addon for Windows Agent.

4 Select the connectors to configure.

5 Specify the location to store events in CEF.

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

6 Specify the values for **File Rotation Interval** and **File Size**.

File Rotation Interval is the interval, in seconds, at which a new file is created. A new file is created when either the File Rotation Interval or the file size exceeds the set value. If the EPS is low in AWS IAM, set the file rotation and file size values lower than the default.

7 Specify the parameters for the selected connectors.

If your connector is	Do this
Dell EMC	Specify the following: ◆ Domain name, hostname, user name, and password ◆ Enable SID Translation
Microsoft Exchange	Specify the following: ◆ Server FQDN ◆ Frequency Set any value between 1 and 600
AWS IAM	Specify the following: ◆ (Optional) Proxy details such as host, port, username, and password ◆ AWS Access Key ◆ AWS Secret Key ◆ AWS SQS URL ◆ AWS SQS Region ◆ AWS SQS Visibility Timeout ◆ AWS SQS Max Received Count ◆ AWS S3 Region
Office 365	Specify the following: ◆ Azure Tenant Domain ◆ Client ID ◆ Client Secret ◆ (Optional) Proxy server, port, username, and password

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

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

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

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

Configuring Change Guardian

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

- "Configuring Memory Settings" on page 39
- "Configuring Server Date and Time Synchronization" on page 39
- "Verifying Server Hostname" on page 39
- "Configuring FIPS 140-2" on page 40
- "Changing Default Email Host Settings" on page 41

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 Sentinel 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 FIPS 140-2

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

To configure Change Guardian to run in FIPS mode:

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

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

---

2 Enable TLS 1.1.

3 (Conditional) If you want to change the keystore password, at the Change Guardian server command prompt, perform the following steps:

3a Switch to `novell` user.

3b Change directory to `/opt/novell/sentinel/bin`, and run the following command:
`chg_keystore_pass.sh`

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

4 Switch to `novell` user.

5 Change directory to `/opt/novell/sentinel/bin`, and run the following command:

```
./convert_to_fips.sh
```

6 Enter the following information:

6a When prompted to backup the server, select `n`.

6b Provide a password that meets the stated criteria. This password is required later during this procedure.

6c (Conditional) If you have created `web server` keystore password in Step 2, specify here.

6d When prompted to enter the external certificate in the keystore database, select n.

6e When prompted to restart the Sentinel server, select y.

7 Ensure that the file `/var/opt/novell/sentinel/log/server0.0.log` contains the following entry:

```
Date_Timestamp|INFO|JAVOS
listener|com.netiq.cg.capi.dao.UpgradeDao.upgrade

Upgrading EventDestination.Upgrade to fips compatible

Date_Timestamp|INFO|JAVOS
listener|com.netiq.cg.capi.dao.UpgradeDao.upgrade

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

8 Change directory to `/opt/netiq/cg/javos/bin`, and run the following command:

```
./convert_to_fips.sh
```

9 Provide the password for the FIPS keystore database (the password you created in Step 6b on page 40).

10 When prompted to restart the javos service, select y.

11 Ensure that the following entry is present in the `javos/log/javos.log` file:

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

12 Change directory to `/opt/netiq/ams/ams/bin`, and run the following command:

```
./convert_to_fips.sh
```

13 Enter the following information:

13a Create the password for the FIPS keystore database.

13b Re-enter the password specified in Step 13a on page 41.

13c When prompted to restart the Agent Manager service, select y.

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

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

Changing Default Email Host Settings

You can change the default Email Host Settings by running the following commands:

1 Change directory:

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

2 Set the email host settings:

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

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

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

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 8443`
- Ensure the appropriate server ports are open:
  - On SLES, run the following command in the server:

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

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

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

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

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

4 Getting Started

This chapter provides the following information:

- “Understanding the Change Guardian Interfaces” on page 43
- “Adding a License Key” on page 45
- “Configuring Security Settings” on page 47
- “Configuring LDAP” on page 50
- “Configuring Users and Roles” on page 53
- “Adding Assets” on page 56

Understanding the Change Guardian Interfaces

Change Guardian provides the following user interfaces:

- Change Guardian Web Console
- Policy Editor

Change Guardian Web Console

The web console includes the following interfaces:

- Change Guardian Dashboard
- Policy Tab
- Agents Tab
- Threat Response Dashboard
- Administration Console

Change Guardian Dashboard

The Change Guardian dashboard provides a quick view of events generated as a result of preconfigured policies. For more information, see “Change Guardian Dashboard ”in the *Change Guardian User Guide*.

Policy

The Policy tab provides reports related to the Change Guardian policies. You can create reports to generate a list of policies that are either not assigned to any agent or are associated with various agents and agent groups.

Adam Mandari is the Change Guardian administrator and is responsible for installing and managing agents. As part of a new setup, Adam deploys Change Guardian agents and creates and assigns policies to the agents. He creates a `Policies not Assigned` report from the Reports tab to identify any policies that are not yet assigned and deletes the policies that are not required anymore.

To be able to email the reports, Adam configures SMTP. He reviews the report and emails the report as PDF from the Policy tab to Daniel Altaner, the architect.

Agents

The Agents tab includes the following interfaces:

- Overview
- Agent Manager

Overview

The Overview dashboard gives you the status of agents in your environment. Based on the heartbeat of agents, the agents are categorized as offline, warning, or online. Agents that have missed a heartbeat goes to offline state through to the next heartbeat poll interval. Agents with warning status displays the reason why they failed to collect events. The dashboard also provides agent details and policies associated with agents. You can configure email IDs to notify users when agents go offline. You can also configure email IDs to send daily updates of the health of agents.

Mandy Rabani is responsible for managing the IT infrastructure in her organization. She is responsible for troubleshooting agent related issues reported by Change Guardian. Mandy cannot spend hours and days to diagnose an issue. She wants to quickly resolve any issues related to Change Guardian agents.

One morning, Mandy finds out that a Change Guardian Agent for Windows is not sending Active Directory events to the Change Guardian server. However, the agent is communicating with the server. To find out the cause of failure, she logs in to the Change Guardian web console and opens the Overview tab. She searches the agent name and clicks on the search result to view the diagnostic report. The last heartbeat was received some time ago and the diagnostic report indicates the issue as “Missing auditing for 'User Account Management', unable to monitor policy”. Using the Overview tab, Mandy quickly identifies and troubleshoot the root cause by configuring auditing on the AD machine. She ensures that Change Guardian is receiving events by logging in to the Change Guardian dashboard. To receive daily health updates of all agents, she configures configures SMTP, sets her email ID, and schedules an email at 9:00 a.m. daily to send her the health status of agents at 9:00 a.m.

NOTE: Upgrade Change Guardian Agent for Windows to 6.0 and Security Agent for UNIX to 7.6.3 to view agent details accurately. Agents that are not upgraded appear offline.

Agent Manager

Agent Manger is a central location where you can manage agents. Agent Manager allows you to deploy and manage your agents directly on the agent host machine, or remotely install agents.

For more information, see the following sections:

- Adding Assets
- Viewing Assets

Alerts

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

Administration

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

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

Policy Editor

Policy Editor allows you to configure and manage policies. You can perform manage application licenses, create and assign policies to assets, create alert rules, configure event destinations, configure emails, schedule monitoring, and so on.

For more information, see the following sections:

- "Adding License for Applications" on page 46
- "Configuring Policies" on page 95
- "Configuring Event Destinations" on page 101
- "Creating and Managing Alert Rules" on page 108
- Chapter 9, "Configuring Email Notifications," on page 113

Adding a License Key

You must add licenses for both the Change Guardian server and applications or modules you plan to monitor.

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

- "Adding the License Key for Server" on page 46
- "Adding License for Applications" on page 46

Adding the License Key for Server

You can either use the Administration Console or the command-line to add the Change Guardian server license key.

- "Adding from the Administration Console" on page 46
- "Adding from the Command Line" on page 46

Adding from the Administration Console

To add a license key using the Administration Console:

1. In the Administration Console, click **About > Licenses**.
2. In the **Licenses** section, click **Add License**.
3. Specify the license key in **Key**.

   NOTE: After a license expires, you can add the license key by using only the command line.

4. Click **Save**.

Adding from the Command Line

To add a license key using the command line:

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

   ```
   su novell
   ```

4. Run the `softwarekey.sh` script:

   ```
   ./softwarekey.sh
   ```

5. Enter 1 to insert the license key.
6. Specify the license key, then press Enter.

Adding License for Applications

Module Manager provides you information about licensed applications and allows you to import application licenses to Policy Editor.

When you install Change Guardian, all available applications are installed automatically on Policy Editor. However, you must add a new application to Policy Editor. To allow Change Guardian to start monitoring, import the license key for each application.

To add a new application to Module Manager:

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

To import a license:

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

2 Select **Module Manager**.

3 Click **Import License Key**.

4 Select the license key for the required application.

Configuring Security Settings

Change Guardian uses the `profile_javos` profile for secure communication.

This section provides the following information:

- "Configuring TLS" on page 47
- "Configuring Certificates" on page 48
- "Applying Updates for Security Vulnerabilities in Embedded Third-Party Products" on page 50

Configuring TLS

Enabling TLS 1.1

By default, TLS 1.1 is disabled for new installations. Enable TLS 1.1 if you have Change Guardian running on FIPS mode.

To enable TLS 1.1:

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

2 Edit the `/opt/novell/sentinel/jdk/jre/lib/security/java.security` file.

3 Remove `TLSv1.1` from the following list of disabled algorithms:

```
jdk.tls.disabledAlgorithms=TLSv1,TLSv1.1,SSLv3, RC4, DES, MD5withRSA,
DH keySize < 1024, EC keySize < 224, 3DES_EDE_CBC, anon, NULL
```

4 Restart the Change Guardian server:

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

Configuring Certificates

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

Following sections provide information about configuring certificates:

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

Installing the Certificates

To install certificates:

1. Log in to the Change Guardian server as `root`.
2. Switch user to `novell`.
3. Go to the `/opt/novell/sentinel/setup` directory.
4. (Optional) Generate request to sign certificate:

   ```
   ./ssl_certs_cg
   ```

   4a. Select **Web Server**.

   4b. Specify the certificate signing request (`.csr`) filename.

   4c. Specify to get the `.csr` file signed by a certificate authority (CA).
5. Copy the CA root certificate chain (`ca.crt`) and the signed certificate (`.crt`) to `/opt/novell/sentinel/setup`.
6. Import the CA root certificate chain and the web server certificate:

   6a. Generate request to sign certificate:

   ```
   ./ssl_certs_cg
   ```

   6b. Select **Import certificate authority root certificate**.

   6c. Enter the CA root certificate chain file name (`ca.crt`).

   6d. Select **Import certificate signed by certificate authority**.

   6e. Select **Web Server**.

   6f. Specify the name of the file that contains the CA signed digital certificate.

   6g. Select another service if necessary or select **Done** and exit from the service option.
7. Select **Exit** to exit from the TLS/SSL certificate configuration.
8. Restart the Change Guardian server:

   ```
   service sentinel restart
   ```
9. Import the CA root certificate change to the computer where you want to use the Administration Console.

Using CA-Signed Certificate

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 LDAP

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

Following sections provide information about configuring LDAP:

- "Configuring LDAP for Authentication" on page 50
- "Configuring LDAP to Access Domain Controller" on page 52

Configuring LDAP for Authentication

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

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

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

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

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

- "Setting up LDAP Authentication" on page 51
- "Logging in Using LDAP User Credentials" on page 52

Setting up LDAP Authentication

To set up LDAP authentication:

1. Log in to the Administration Console, click **Users > LDAP Settings**.
2. Specify the options to configure LDAP authentication:

   Host: Hostname or IP address for SSL connections.

   SSL: SSL connection to the LDAP server.

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

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

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

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

   Base DN: The root container to search for users.

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

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

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

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

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

   Domain Name: The Active Directory domain.

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

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

   For example, if the Base DN is set to `o=netiq` and the absolute user DN is `cn=sentinel_ldap_user,o=netiq`, Change Guardian uses the relative user DN `cn=sentinel_ldap_user` when you create an LDAP user account.

   ---

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

- Any one of the following characters: +, ", \, <, >, or ;

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

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

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

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

---

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

Verify the configuration:

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

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

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

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

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

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

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

Logging in Using LDAP User Credentials

After configuring the Change Guardian server for LDAP authentication, create Change Guardian LDAP user accounts and log in to Change Guardian by using your LDAP user name and password. For more information about creating LDAP user accounts, see "Creating Users" on page 56.

Configuring LDAP to Access Domain Controller

To access and configure the domain controller in LDAP settings:

1 In Policy Editor, click **Settings > LDAP Settings**.

2 In the LDAP Settings window, click **New**.

3 Specify the following fields:

Domain name: Name of the Active Directory domain.

For example, `test.example.com`

User name: Name of the Active Directory user name.

You can specify the user name in the following format:

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

Password: Password for the Active Directory user.

Polling interval: The interval at which the Change Guardian server synchronizes all objects and entities with Active Directory configuration.

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

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

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

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

Configuring Users and Roles

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

Following sections provide information about configuring users and roles:

- "Overview" on page 53
- "Creating Roles" on page 54
- "Understanding Password Complexity" on page 55
- "Creating Users" on page 56

Overview

Change Guardian has the following roles by default:

Administrator: A user in this role has administrative rights in Change Guardian. Administrative rights include the ability to perform user administration, data collection, data storage, search operations, rules, report, dashboard, and license management.

You cannot modify or delete the administrator role.

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

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

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

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

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

Creating Roles

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

To create a role, log in to the Administration Console and click **Users > Users and Roles**. Under **Roles**, click **Create**. Review the following additional roles that you can assign to the new role:

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

  ---

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

- **View and execute event actions:** Allows members to view events and execute actions on the selected events
- **View detailed internal system state data:** Allows members to view detailed internal system state data by using a JMX client
- **View knowledge base:** Allows users to view the knowledge base in the **Alert Details** page

To create users, see “Creating Users” on page 56.

Understanding Password Complexity

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

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

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

The following table describes the password complexity validation rules:

Table 4-1 *Password Complexity Rules*

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

Validation Rule	Description
RESTRICTED_WORDS_IN_PASSWORD	Specifies the words that are not allowed in a password. The restricted words are case-insensitive. You can specify multiple words separated by a comma. For example, `RESTRICTED_WORDS_IN_PASSWORD= admin, password, test`

Creating Users

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

To create a user, log in to the Administration Console and click **Users > Users and Roles**. You can use special characters to set the user name. However, the user name should be within 30 characters.

If you want the server to authenticate the user against the internal database, select the default authentication method **Local**. However, if you want the server to authenticate the user against an LDAP directory, select **Directory**. **Directory** is enabled only if you have configured the Change Guardian server for LDAP authentication. For more information, see "Configuring LDAP for Authentication" on page 50.

NOTE: For local user password, ensure that the password adheres to the password complexity validation rules. For more information, see "Understanding Password Complexity" on page 55.

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 receive events, you must first add assets.

This section provides information about the following:

- "Adding Assets" on page 56
- "Viewing Assets in Agent Manager" on page 57
- "Viewing Assets in Policy Editor" on page 57

Adding Assets

To add assets in Agent Manager:

1. Log in to Change Guardian, click **Integration > Agent Manager**.
2. (Conditional) To add the first asset, click **All Assets > Manage Assets > Add**.

3 (Conditional) To add additional assets, click **Asset Groups > All Assets > Add Assets**.

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

NOTE: If you are using Active Directory over SSL or TLS connection, ensure that you have imported the Active Directory SSL certificate to the Change Guardian server. For more information, see "Configuring Certificates" on page 48.

---

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

Create a text file with a header line containing the columns Hostname, MajorType, and Addresses, 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.

Viewing Assets in Agent Manager

Agent Manager displays assets in the following asset groups:

All Assets: Assets added or imported to Agent Manager.

Approved Assets: Assets to which Agent Manager successfully deployed a Change Guardian agent.

You have to authenticate an asset once after installing an agent.

Assets that have not communicated: Assets in which Client Agent Manager service cannot communicate with the Agent Management Service.

To move an asset to **Approved asset**, check whether the Client Agent Manager service is communicating with Agent Management Service.

Assets not in any group: Assets in which Agent Manager installed an agent, but they are not part of user-defined group.

To move assets from this group to any user defined group, select the asset, go to **Manage Asset > Move Assets to a Group**, and then select the required group.

User defined groups: A list of user defined groups and user-defined categories.

To organize and manage assets, you can create asset groups under **User defined groups** and copy assets from **Approved Assets** group to **User defined groups**.

Viewing Assets in Policy Editor

In Policy Editor, 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.

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.

- **Static groups:** Assets you manually add.

  To add or remove members, manually update the group.
- **Dynamic groups:** Assets that match the filter criteria you specify for the group.

Policy Editor does not show an asset group if the group does not contain registered assets.

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

5 Configuring Event Monitoring

Change Guardian monitors events of your assets such as Windows Active Directory, Group Policy, Windows, and so on.

This section provides information about configuring the following assets:

- "Configuring Windows Active Directory Monitoring" on page 59
- "Configuring Group Policy Monitoring" on page 65
- "Configuring Windows Monitoring" on page 69
- "Configuring Microsoft Azure Active Directory Monitoring" on page 70
- "Configuring AWS Identity and Access Management" on page 76
- "Configuring Office 365 Monitoring" on page 79
- "Configuring Dell EMC Monitoring" on page 81
- "Configuring Microsoft Exchange Monitoring" on page 83
- "Configuring NetApp Storage Monitoring" on page 86
- "Configuring Linux or UNIX Monitoring" on page 91

Configuring Windows Active Directory Monitoring

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

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

This chapter provides information about the following:

- "Implementation Checklist" on page 60
- "Prerequisites" on page 60
- "Configuring Active Directory" on page 60
- "Categories of Windows Active Directory Policies" on page 64

Implementation Checklist

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

Task	See
Review requirements and recommendations for computers running the AD Domain Service	Change Guardian System Requirements
Complete the prerequisites	"Prerequisites" on page 60
Add the license key	"Adding a License Key" on page 45
Configure Windows Active Directory	"Configuring the Security Event Log" on page 61
	"Configuring AD Auditing" on page 61
	"Configuring User and Group Auditing" on page 62
	"Configuring Security Access Control Lists" on page 63
	"Synchronizing Active Directory User Accounts" on page 128
Configure Change Guardian for monitoring	"Categories of Windows Active Directory Policies" on page 64
	"Assigning Policies and Policy Sets" on page 98
Triage events	Chapter 7, "Managing Events," on page 101
	Chapter 8, "Configuring Alerts," on page 107

Prerequisites

Ensure that you have completed the following:

- Install Change Guardian Agent for Windows
- Install Policy Editor

Configuring Active Directory

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

- "Configuring the Security Event Log" on page 61
- "Configuring AD Auditing" on page 61
- "Configuring User and Group Auditing" on page 62
- "Configuring Security Access Control Lists" on page 63

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

Configuring the Security Event Log

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

To configure the security event log:

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

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

5. Expand **Computer Configuration > Policies > Windows Settings > Security Settings**.
6. Select **Event Log** and set:
   - **Maximum security log size** to 10240 KB (10 MB) or more
   - **Retention method for security log** to **Overwrite events as needed**
7. To update policy settings, run the `gpUpdate` command at the command prompt.

To verify the configuration is successful:

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

Configuring AD Auditing

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

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

To configure AD auditing:

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

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

5. Expand **Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies**.
6. Under **Account Management**, and **Policy Change**, select the following for each subcategory: **Configure the following audit events**, **Success**, and **Failure**.
7. Click **Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options,** enable **Force audit policy subcategory setting on the default domain policy**.
8. Under **Windows Settings > Security Settings**, expand **Local Policies > Audit Policy**.
9. Under **Audit account management**, **Audit directory service access**, and **Audit policy change**, select the following for each subcategory: **Define these policy settings**, **Success**, and **Failure**.
10. To set audit policy using group policies, expand **Computer Configuration > Windows Settings > Security Settings > Local Policies > Audit Policy.**
11. Select **Define these policy settings**, **Success**, and **Failure**.
12. To update policy settings, run the `gpUpdate` command at the command prompt.

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

Configuring User and Group Auditing

Configure user and group auditing to audit the following activities:

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

To configure user and group auditing:

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

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

10 Under **Audit Logon**, select **Audit Logon**, **Success**, and **Failure**.

11 Under **Audit Logoff**, select **Audit Logoff**, **Success**, and **Failure**.

12 To update policy settings, run the `gpupdate /force` command at the command prompt.

Configuring Security Access Control Lists

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

To allow Change Guardian to monitor changes of current and future objects inside Active Directory, follow the steps in "Configuring SACLs for AD" on page 63. However, if you are using Change Guardian for only Group Policy in your environment, see "Configuring SACLs for GPO" on page 67.

Configuring SACLs for AD

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

To configure SACLs:

1 Log in as an administrator to a computer in the domain that you want to configure.

2 To open ADSI Edit configuration tool, run `adsiedit.msc` at the command prompt.

3 Right-click **ADSI Edit**, and select **Connect to**.

4 In the Connection Settings window, specify the following:

- **Name** as `Default naming context`.
- **Path** to the domain to configure.
- If you are performing this step for the first time, select **Default naming context**.
- If you are performing for the second time, select **Schema.**
- If you are performing for the third time, select **Configuration**.

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

---

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

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

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

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

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

10 Configure auditing to monitor every user:

Condition	Task
If you are using Windows Server 2012 or later	1. Click **Select a principal**, and type `everyone` in **Enter the object name to select**. 2. Specify the following options: ◆ **Type** as **All** ◆ Select **Permissions** as: ◆ **Write All Properties** ◆ **Delete** ◆ **Modify Permissions** ◆ **Modify Owner** ◆ **Create All Child Objects** The other nodes related to child objects are selected automatically ◆ **Delete All Child Objects** The other nodes related to child objects are selected automatically
For Windows versions lower than 2012	1. Type `everyone` in **Enter the object name to select**. 2. Under **Permissions**, select **Successful** and **Failed** for the following: ◆ **Write All Properties** ◆ **Delete** ◆ **Modify Permissions** ◆ **Modify Owner** ◆ **Create All Child Objects** The other nodes related to child objects are selected automatically ◆ **Delete All Child Objects** The other nodes related to child objects are selected automatically

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

12 Repeat Step 4 through Step 11 two more times.

Categories of Windows Active Directory Policies

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

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

Configurations: Policies about creating and deleting GPOs

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

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

Groups: Policies about the following:

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

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

Schema: Policies about the following:

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

Trusts: Policies about creating, deleting, and modifying trust

User accounts: Policies about the following:

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

For more information about creating policies, see "Creating Change Guardian Policies" on page 96.

After creating policies, you can assign them to assets. For information about assigning policies, see "Working with Policies" on page 97.

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

Configuring Group Policy Monitoring

Change Guardian monitors the following in Group Policy:

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

This section provides the following information:

- "Implementation Checklist" on page 66
- "Prerequisites" on page 66
- "Configuring GPO" on page 66
- "Categories of GPO Policies" on page 68

Implementation Checklist

Complete the following tasks to start monitoring Group Policy events:

Task	See
Complete the prerequisites	"Prerequisites" on page 66
Add the license key	"Adding a License Key" on page 45
Configure Change Guardian for monitoring	"Configuring the Security Event Log" on page 61
	"Configuring AD Auditing" on page 61
	"Configuring SACLs for GPO" on page 67
	"Categories of GPO Policies" on page 68
Triage events	Chapter 7, "Managing Events," on page 101
	Chapter 8, "Configuring Alerts," on page 107

Prerequisites

Ensure that you have completed the following:

- Install Change Guardian Agent for Windows
- Install Policy Editor

Configuring GPO

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

- "Configuring the Security Event Log" on page 61
- "Configuring AD Auditing" on page 61
- "Configuring SACLs for GPO" on page 67

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

Configuring SACLs for GPO

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

To configuration SACL:

1. Log in as an administrator to the computer in the domain you want to configure.
2. To open ADSI Edit configuration tool, run `adsiedit.msc` at the command prompt.
3. Right-click **ADSI Edit**, and then select **Connect to**.
4. In the Connection Settings window, specify the following:
   - **Name** as `Default naming context`.
   - **Path** to the domain to configure.
5. In **Connection Point**, set **Select a well known Naming Context** to **Default naming context**.
6. In the ADSI Edit window, expand **Default naming context**.
7. Right-click the node under the connection point (begins with DC=), and select **Properties**.
8. On the **Security** tab, click **Advanced > Auditing > Add**.
9. Deselect the option **Apply these auditing entries to objects and/or containers within this container only**.
10. Configure auditing to monitor every user:

Condition	Task
If you are using Windows Server 2012 or later	1. Click **Select a principal** and type `everyone` in **Enter the object name to select**. 2. Specify the following options: ◆ **Type** as **All** ◆ Select **Permissions** as: ◆◆ **Delete** ◆◆ **Create Organizational Unit objects** ◆ Select **Properties** as: ◆◆ **Write gPLink** ◆◆ **Write gPOptions**
For Windows versions lower than 2012	1. Type `everyone` in the **Enter the object name to select** field. 2. Select **Permissions** as: ◆ **Delete** ◆ **Create Sites Container objects** 3. Select **Properties** as: ◆ **Write gPLink** ◆ **Write gPOptions**

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

12 Expand **Configuration**.

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

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

15 Configure auditing to monitor every user:

Condition	Task
If you are using Windows Server 2012 or later	1. Click **Select a principal** and type `everyone` in **Enter the object name to select**. 2. Specify the following options: ◆ **Type** as **All** ◆ Select **Permissions** as: ◆ **Delete** ◆ **Create Organizational Unit objects** ◆ Select **Properties** as: ◆ **Write gPLink** ◆ **Write gPOptions**
For Windows versions lower than 2012	1. Type `everyone` in the **Enter the object name to select** field. 2. Select **Permissions** as: ◆ **Delete** ◆ **Create Sites Container objects** 3. Select **Properties** as: ◆ **Write gPLink** ◆ **Write gPOptions**

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

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

Categories of GPO Policies

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

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

Group Policy Settings: Policies about modifying software settings

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

SYSVOL: Policies about changing Central Store and SYSVOL folder

For information about creating policies, see "Creating Change Guardian Policies" on page 96.

After creating policies, you can assign them to assets. For information about assigning policies, see "Working with Policies" on page 97.

Configuring Windows Monitoring

Change Guardian monitors the following in Windows:

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

This section provides the following information:

- "Implementation Checklist" on page 69
- "Prerequisites" on page 69
- "Categories of Windows Policies" on page 69

Implementation Checklist

Complete the following tasks to start monitoring Windows events:

Task	See
Complete the prerequisites	"Prerequisites" on page 69
Add a license key	"Adding a License Key" on page 45
Configure Change Guardian for monitoring	"Categories of Windows Policies" on page 69
	"Assigning Policies and Policy Sets" on page 98
Triage events	Chapter 7, "Managing Events," on page 101
	Chapter 8, "Configuring Alerts," on page 107

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 Windows Policies

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\repositoryEnable\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 Change Guardian Policies" on page 96.

After creating policies, you can assign them to assets. For information about assigning policies, see "Working with Policies" on page 97.

Configuring Microsoft Azure Active Directory Monitoring

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

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

Change Guardian monitors the following in Azure AD:

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

This section provide the following information:

- “Implementation Checklist” on page 71
- “Prerequisites” on page 72
- “Configuring Default Windows Registry Keys” on page 73
- “Configuring Change Guardian for Monitoring” on page 74
- “Categories of Azure AD Policies” on page 75
- “Troubleshooting” on page 76

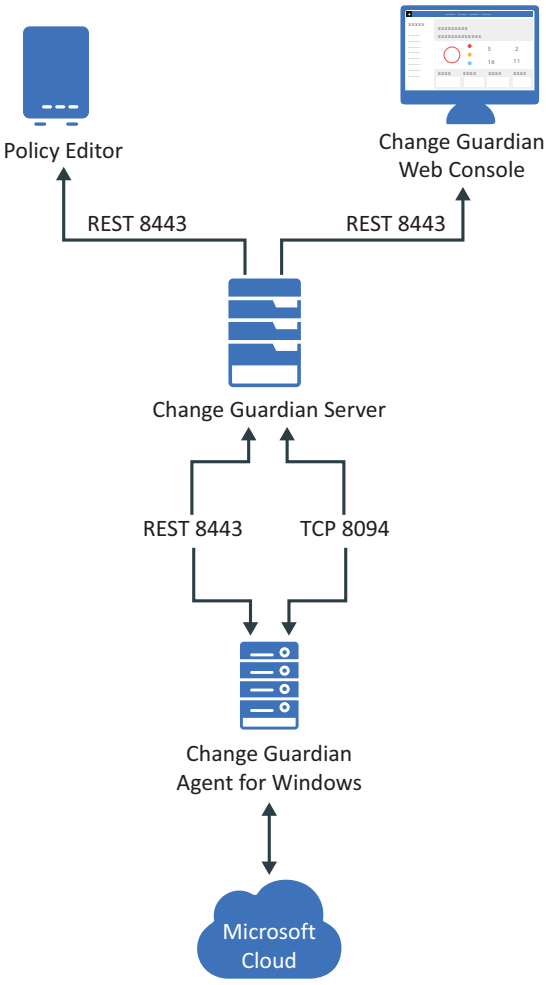
Implementation Checklist

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

Task	See
Complete the prerequisites	“Prerequisites” on page 72
Ensure that you have created a tenant and that its credentials are available for Change Guardian. Required credential details: ◆ Domain Name ◆ Authentication Key ◆ Application ID	Microsoft Azure AD portal
Add the license key	“Adding a License Key” on page 45
(Conditional) If you want to modify the default keys based on your requirements, configure the default Windows registry keys.	“Configuring Default Windows Registry Keys” on page 73
Configure Change Guardian for monitoring.	“Enabling Azure AD Monitoring” on page 74 “Configuring Azure AD Tenant” on page 75 “Categories of Azure AD Policies” on page 75 “Assigning Policies and Policy Sets” on page 98
(Conditional) If you have upgraded Change Guardian, ensure that you reconfigure the Change Guardian Agent for Windows to enable Azure AD monitoring.	“Enabling Azure AD Monitoring” on page 74
Triage events.	Chapter 7, “Managing Events,” on page 101 Chapter 8, “Configuring Alerts,” on page 107

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

Figure 5-1 *Azure AD Monitoring using Change Guardian*



The deployment diagram illustrates the following:

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

Prerequisites

Ensure that you have completed the following:

- Install Change Guardian Agent for Windows
- Install Policy Editor

Configuring Default Windows Registry Keys

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

- "Configuring Azure AD Event Fetching Interval" on page 73
- "Configuring Azure AD Access Token Refresh Time Interval" on page 73
- "Configuring Azure AD Event Collection Interval" on page 74

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

Configuring Azure AD Event Fetching Interval

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

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

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

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

To modify the time interval:

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

Configuring Azure AD Access Token Refresh Time Interval

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

To modify the time interval:

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

Configuring Azure AD Event Collection Interval

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

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

To modify this time interval:

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

Configuring Change Guardian for Monitoring

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

- “Enabling Azure AD Monitoring” on page 74
- “Configuring Azure AD Tenant” on page 75

Enabling Azure AD Monitoring

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

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

To reconfigure:

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

Configuring Azure AD Tenant

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

To configure the Azure AD tenant:

1. Log in to Policy Editor.
2. Under **Azure AD**, open **Azure Tenant Configuration**.
3. Specify values for the following fields:
   - **Domain Name**: Specify the name of the Azure AD domain.
   - **Application ID**: Enter the Application ID that was displayed in the Azure portal during configuration.
   - **Authentication Key**: Enter the Authentication Key that was displayed in the Azure portal during configuration.

Categories of Azure AD Policies

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

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

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

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

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

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

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

For information about creating Azure AD policies, see “Creating a Policy for Azure AD Groups” on page 75. For information about creating policies in Change Guardian, see “Creating Change Guardian Policies” on page 96.

After creating policies, you can assign them to assets. For information about assigning policies, see “Working with Policies” on page 97.

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

Creating a Policy for Azure AD Groups

To create a policy:

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

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

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

Troubleshooting

This section contains some issues you might experience while monitoring Azure AD, along with their workarounds.

Change Guardian Receives an Insufficient Access Permission event

Issue: Change Guardian receives Insufficient Access Permission event because *Read directory data* permissions are not assigned to the Azure AD web application for both Application and Delegated permission types.

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

Change Guardian Receives an Invalid Configuration event

Issue: Change Guardian receives Invalid Configuration event because of the incorrect Domain Name, Authentication Key, or Application ID used to access Azure AD.

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

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

Change Guardian Is Unable to Receive Azure AD Events

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

- Tenant is not reachable
- Invalid remote web application

Workaround:

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

Configuring AWS Identity and Access Management

Change Guardian monitors the following in AWS IAM:

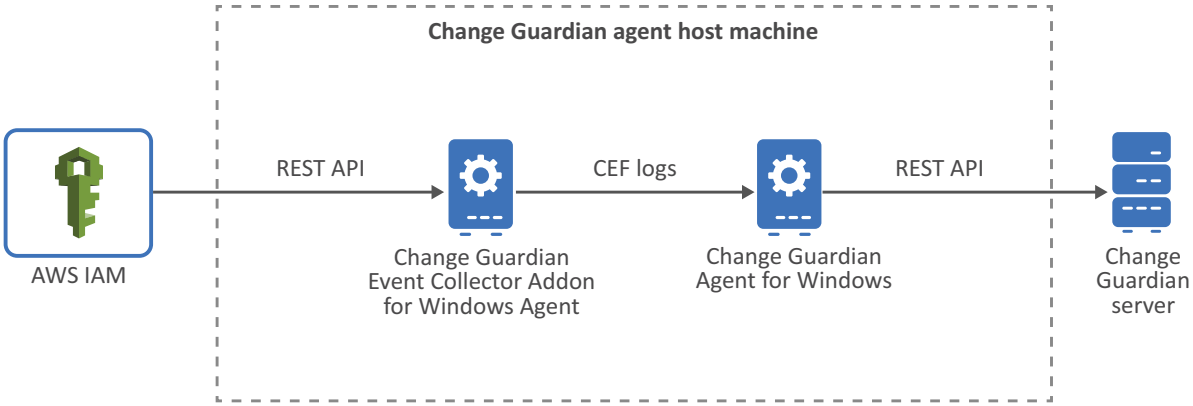
- Access Control
- Groups
- Identity and Profiling

- Policies
- User Accounts

This section provides the following information:

- “Implementation Checklist” on page 77
- “Prerequisites” on page 77
- “Configuring Change Guardian for Monitoring” on page 78
- “Categories of AWS IAM Policies” on page 78

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



Implementation Checklist

Complete the following tasks to start monitoring AWS IAM events:

Task	See
Complete the prerequisites	“Prerequisites” on page 77
Add the license key	“Adding a License Key” on page 45
Configure Change Guardian for monitoring	“Configuring Change Guardian for Monitoring” on page 78
Triage events	Chapter 7, “Managing Events,” on page 101
	Chapter 8, “Configuring Alerts,” on page 107

Prerequisites

Ensure that the following is complete:

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

Configuring Change Guardian for Monitoring

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

Enabling AWS IAM Monitoring

To enable monitoring:

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

   Or

   In Agent Manager, select the asset and click **Manage Installations > Reconfigure Agents.**
2. In the Reconfigure Agent page, select **Enable Collector Plugin** under **Edit Agent Configuration**.
3. Specify the location to store CEF events in **CEF Data Output Path**.

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

Categories of AWS IAM Policies

Access Control: Policies about the following:

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

Groups: Polices about creating, changing, and deleting groups

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

Policies: Policies about the following:

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

User Accounts: Policies about the following:

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

For information about creating policies in Change Guardian, see "Creating Change Guardian Policies" on page 96.

After creating policies, you can assign them to assets. For information about assigning policies, see "Working with Policies" on page 97.

Configuring Office 365 Monitoring

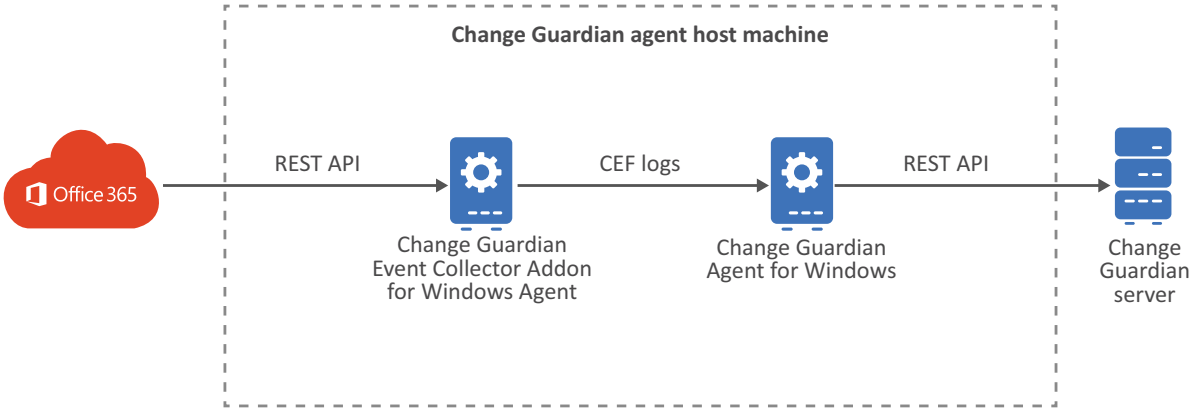
Change Guardian monitors the following in Office 365:

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

This section provides the following information:

- "Implementation Checklist" on page 79
- "Prerequisites" on page 80
- "Configuring Change Guardian for Monitoring" on page 80
- "Categories of Office 365 Policies" on page 80

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



Implementation Checklist

Complete the following tasks to start monitoring Office 365 events:

Task	See
Complete the prerequisites	"Prerequisites" on page 80
Add the license key	"Adding a License Key" on page 45
Configure Change Guardian for monitoring	"Configuring Change Guardian for Monitoring" on page 80
Triage events	Chapter 7, "Managing Events," on page 101
	Chapter 8, "Configuring Alerts," on page 107

Prerequisites

Ensure that the following is complete:

- Setting Up Office 365
- Install Change Guardian Event Collector Addon for Windows Agent
- Install Change Guardian Agent for Windows
- Install Policy Editor

Configuring Change Guardian for Monitoring

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

Enabling Office 365 Monitoring

To enable monitoring:

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

   Or

   In Agent Manager, select the asset and click **Manage Installations > Reconfigure Agents.**
2. In the Reconfigure Agent page, select **Enable Collector Plugin** under **Edit Agent Configuration**.
3. Specify the location to store CEF events in **CEF Data Output Path**.

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

Categories of Office 365 Policies

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

Mailbox Accounts: Policies about the following:

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

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

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

For information about creating policies in Change Guardian, see "Creating Change Guardian Policies" on page 96.

After creating policies, you can assign them to assets. For information about assigning policies, see “Working with Policies” on page 97.

Configuring Dell EMC Monitoring

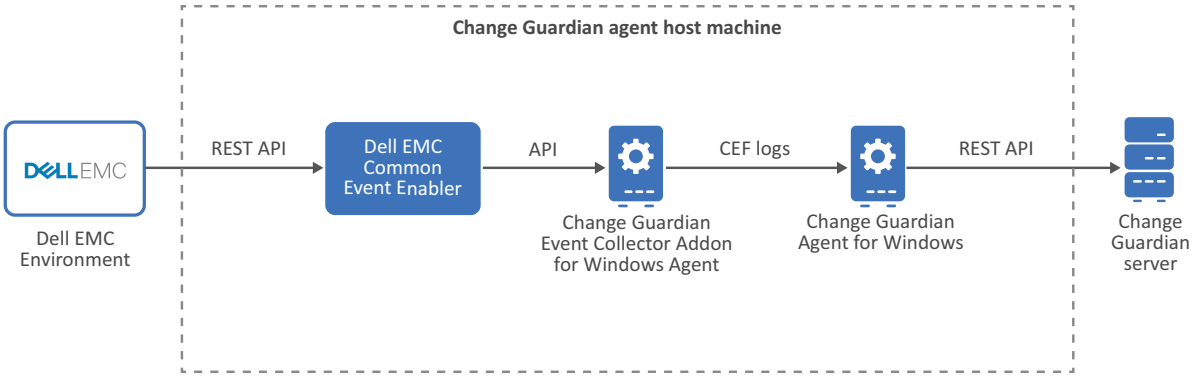
Change Guardian monitors Dell EMC file systems on Isilon and Unity storage platforms.

This section provides the following information:

- “Implementation Checklist” on page 81
- “Prerequisites” on page 82
- “Configuring Change Guardian for Monitoring” on page 82
- “Categories of Dell EMC Policies” on page 83

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

Figure 5-2 *Dell EMC Monitoring using Change Guardian*



The deployment diagram illustrates the following:

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

Implementation Checklist

Complete the following tasks to start monitoring Dell EMC events:

Task	See
Complete the prerequisites	"Prerequisites" on page 82
Add a license key	"Adding a License Key" on page 45
Configure Change Guardian for Dell EMC monitoring	"Configuring Change Guardian for Monitoring" on page 82
	"Working with Policies" on page 97
Triage events	Chapter 7, "Managing Events," on page 101
	Chapter 8, "Configuring Alerts," on page 107

Prerequisites

Ensure that you have completed the following:

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

Configuring Change Guardian for Monitoring

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

Enabling Dell EMC Monitoring

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

To enable monitoring:

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

   Or

   In Agent Manager, select the asset and click **Manage Installations > Reconfigure Agents.**
2. In the Reconfigure Agent page, select **Enable Collector Plugin** under **Edit Agent Configuration**.
3. Specify the location to store CEF events in **CEF Data Output Path**.

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

Categories of Dell EMC Policies

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

For information about creating policies, see "Creating Change Guardian Policies" on page 96.

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

For example,

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

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

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

After creating policies, you can assign them to assets. For information about assigning policies, see "Working with Policies" on page 97.

Configuring Microsoft Exchange Monitoring

Change Guardian monitors the following in Microsoft Exchange:

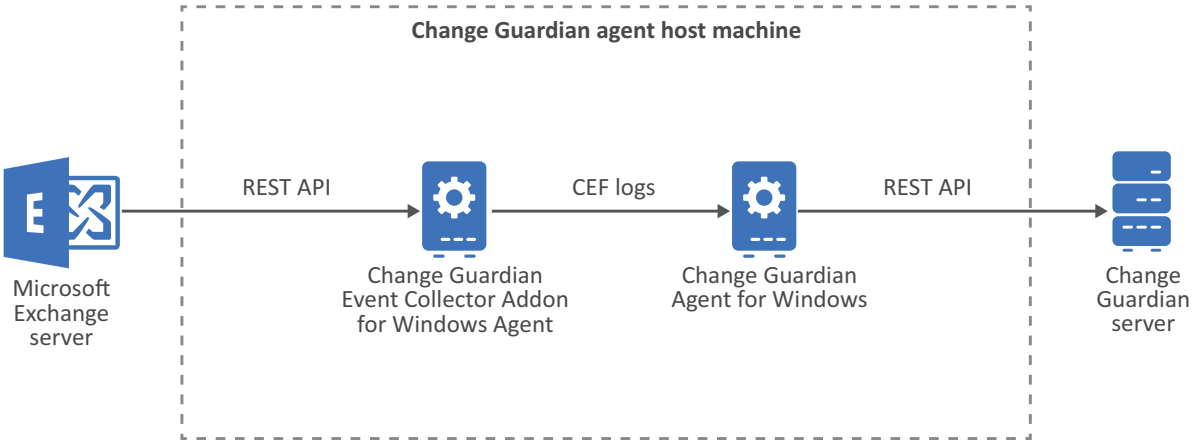
- Exchange Settings
- Mailbox Accounts
- Mailbox Messages
- Management Role Groups

This section provides the following information:

- "Implementation Checklist" on page 84
- "Prerequisites" on page 84
- "Configuring Change Guardian for Monitoring" on page 85
- "Categories of Microsoft Exchange Policies" on page 85

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

Figure 5-3 *Microsoft Exchange Monitoring using Change Guardian*



The deployment diagram illustrates the following:

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

Implementation Checklist

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

Task	See
Complete the prerequisites	“Prerequisites” on page 84
Add the license key	“Adding a License Key” on page 45
Configure Change Guardian for monitoring	“Enabling Exchange Monitoring” on page 85 “Categories of Microsoft Exchange Policies” on page 85
Triage events	Chapter 7, “Managing Events,” on page 101 Chapter 8, “Configuring Alerts,” on page 107

Prerequisites

Complete the following tasks in the same order:

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

1. Setting Up Exchange

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

Configuring Change Guardian for Monitoring

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

Enabling Exchange Monitoring

Ensure that you have added Exchange assets in Agent Manager.

To enable monitoring:

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

Or

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

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

3 Specify the location to store CEF events in **CEF Data Output Path**.

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

Categories of Microsoft Exchange Policies

Exchange Settings: Policies about creating and deleting configuration settings

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

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

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

For information about creating policies, see “Creating Change Guardian Policies” on page 96.

After creating policies, you can assign them to assets. For information about assigning policies, see “Working with Policies” on page 97.

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

Configuring NetApp Storage Monitoring

Storage solutions such as NetApp store a large amount of data and, therefore, can have a large volume of audit events. You can monitor and receive alerts for a variety of malicious behaviors that occur on a Network Attached Storage (NAS) device. For example, unauthorized user accessing confidential files and directories. You can also include or exclude certain files from the audit scope to ensure a faster and more efficient audit process.

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

- "Implementation Checklist" on page 86
- "Prerequisites" on page 86
- "Configuring the NetApp Native Auditing" on page 87
- "Configuring Change Guardian for Monitoring" on page 89
- "Categories of NetApp Policies" on page 91

Implementation Checklist

Complete the following tasks to start monitoring NetApp events:

Task	See
Complete the prerequisites	"Prerequisites" on page 86
Add a license key	"Adding a License Key" on page 45
Configure NetApp native auditing	"Configuring NetApp Native Auditing for CIFS" on page 87
	"Configuring NetApp Native Auditing for NFS" on page 88
Configure Change Guardian for NetApp monitoring	"Mounting the Audit Logs in CIFS" on page 90
	"Mounting the Audit Logs in NFS" on page 90
	"Creating a Configuration File" on page 91
Triage events	Chapter 7, "Managing Events," on page 101
	Chapter 8, "Configuring Alerts," on page 107

Prerequisites

Ensure that you have completed the following:

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

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

- Install Policy Editor

Configuring the NetApp Native Auditing

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

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

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

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

Configure NetApp auditing depending on the filesystem it uses:

- "Configuring NetApp Native Auditing for CIFS" on page 87
- "Configuring NetApp Native Auditing for NFS" on page 88

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

Configuring NetApp Native Auditing for CIFS

Create an auditing configuration on the given SVM for CIFS before you can monitor events on NetApp storage. You can monitor these events on CIFS by setting SACLs on storage objects in NTFS or mixed mode volumes.

To configure auditing for CIFS:

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

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

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

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

3. Verify audit configuration:

   ```
   vserver audit show -vserver <Name_SVM>
   ```

   For example, to verify audit configuration for SVM1, run the following command:

   ```
   vserver audit show -vserver SVM1
   ```

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

4 Enable SVM auditing:

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

Example:

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

Configuring NetApp Native Auditing for NFS

To configure auditing in NFS:

1 Launch the Data ONTAP command-line interface.

2 Create audit configuration for an SVM:

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

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

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

3 Verify audit configuration:

```
vserver audit show -vserver <Name_SVM>
```

For example, to verify audit configuration for SVM1, run the following command:

```
vserver audit show –vserver SVM1
```

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

4 Enable SVM auditing:

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

Example:

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

5 To configure Security Agent for UNIX to monitor the NetApp filesystem changes, enable ACL for NFS:

```
vserver nfs modify -vserver <name_SVM> -v4.0 enabled -v4.0-acl enabled
```

Example:

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

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

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

6b Mount to the directory:

```
mount -t nfs4 <nas_SVMIP>:/<volume_name> <mount_path>
```

Example:

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

```
mount -t nfs4 x.x.x.x:/vol1 /mnt/folder1
```

6c To monitor each folder within a volume, add audit flags recursively on each folder in the mount directory you want to monitor:

```
nfs4_setfacl -R -a U:fdSF:EVERYONE@:rwaDdTNCo <NFS_Share>
```

Example:

If a folder name in the volume is `NFSShare`, run the following command:

```
nfs4_setfacl -R -a U:fdSF:EVERYONE@:rwaDdTNCo NFSShare
```

6d To monitor an entire volume, add audit flags recursively on the mount directory that contains the volume mounted:

```
nfs4_setfacl -R -a U:fdSF:EVERYONE@:rwaDdTNCo <mount directory>
```

Example:

If the mount directory is `/mnt/folder1`, run the following command:

```
nfs4_setfacl -R -a U:fdSF:EVERYONE@:rwaDdTNCo /mnt/folder1
```

Configuring Change Guardian for Monitoring

After configuring NetApp audit, mount the NetApp volumes into Security Agent for UNIX. Mount one volume for audit logs and another for CIFS or NFS shares to monitor.

Complete the following tasks to configure Change Guardian:

- “Mounting the Audit Logs in CIFS” on page 90
- “Mounting the Audit Logs in NFS” on page 90
- “Creating a Configuration File” on page 91

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

Mounting the Audit Logs in CIFS

To mount the audit log:

1. Create a mount directory.

   Example:

   `mkdir /mnt/audit`

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

   `username=<user name>`

   `password=<password>`

   `domain=<domain name>`

4. Change the permissions of this file to secure its credentials:

   `chmod 600 cifs`

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

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

   Example:

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

6. Mount the audit volume to the mount location:

   `mount /mnt/audit`

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

Mounting the Audit Logs in NFS

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

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

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

   Example:

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

3. Mount the audit volume to the mount location:

   `mkdir /mnt/audit`

NOTE: Make changes to `/etc/fstab` and mount the volume with the NetApp share following the above steps.

Creating a Configuration File

Complete the following steps in the Security Agent for UNIX machine:

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

   `SVM_IP_address, share, mount_directory, volume`

   Example:

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

   `x.x.x.x,/vol1,/mnt/audit,vol1`

NOTE: When you monitor an entire volume, you must update the NetApp volume tab as follows:

`x.x.x.x,/vol1,/mnt/audit,vol1`

Categories of NetApp Policies

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

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

For information about creating policies, see "Creating Change Guardian Policies" on page 96.

After creating policies, you can assign them to assets. For information about assigning policies, see "Working with Policies" on page 97.

Configuring Linux or UNIX Monitoring

Change Guardian monitors the following in Linux and UNIX environments:

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

This section provides the following information:

- "Implementation Checklist" on page 92
- "Prerequisites" on page 92
- "Categories of UNIX Policies" on page 92

Implementation Checklist

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

Task	See
Complete the prerequisites	"Prerequisites" on page 92
Add a license key	"Adding a License Key" on page 45
Configure Change Guardian for monitoring	"Categories of UNIX Policies" on page 92
	"Assigning Policies and Policy Sets" on page 98
Triage events	Chapter 7, "Managing Events," on page 101
	Chapter 8, "Configuring Alerts," on page 107

Prerequisites

Ensure that you have completed the following:

- Install Security Agent for UNIX
- Configure Security Agent for UNIX
- Install Policy Editor

Categories of UNIX Policies

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 Security Agent for UNIX configuration and system message of the day

File System: Policies to monitor bash shell startup configuration

Groups: Policies to monitor inbuilt groups

Mount: Policies to monitor CD-ROM mounts

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

Users: Policies to monitor built-in users

For information about creating policies, see “Creating Change Guardian Policies” on page 96.

After creating policies, you can assign them to assets. For information about assigning policies, see “Working with Policies” on page 97.

6 Configuring 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.

- "Understanding Policies and Policy Sets" on page 95
- "Creating Change Guardian Policies" on page 96
- "Working with Policies" on page 97
- "Policy Reports" on page 100

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 can combine multiple policies from one or more assets to organize and manage monitoring the assets. 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 Security 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 settings for every grouped resource. 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. You can also browse Active Directory items for a policy.

Creating Change Guardian Policies

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

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

Creating a Fresh Policy

You can create a fresh policy without preconfigured settings.

To create a policy:

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

NOTE: For more information about enabling a policy, see "Enabling a Change Guardian Policy Revision" on page 98.

Working with Policies

Change Guardian stores the policies in the Change Guardian policy repository. You can assign policies to assets or asset groups.

After creating a policy, you can perform various activities such as clone a policy, assign the policy to an asset, 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
3. Assign a policy revision to an asset or asset group

This section provides the following information:

- "Cloning a Change Guardian Policy" on page 97
- "Creating Change Guardian Policy Sets" on page 98
- "Assigning Policies and Policy Sets" on page 98
- "Enabling a Change Guardian Policy Revision" on page 98
- "Exporting and Importing Change Guardian Policies" on page 99
- "Assigning Event Destinations to Change Guardian Policies" on page 99
- "Scheduling Change Guardian Policy Monitoring" on page 99

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 assets 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 98.

Creating Change Guardian Policy Sets

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

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

Assigning Policies and Policy Sets

When you select an asset or asset group in Policy Editor, you can view the policies and policy sets assigned to it. You can assign additional policies and policy sets to an asset.

To assign a policy or policy set to an asset:

1. Click **Change Guardian > Policy Assignment**.
2. Select an asset or asset group, and click **Assign Policies**.
3. Select a policy set or policy, and click **Apply**.

NOTE: You cannot assign policies using **Asset Groups** for the following asset types: Azure AD, AWS for IAM, Dell EMC, Microsoft Exchange, Microsoft Office 365, and NetApp.

You can edit an existing policy or policy set from the way it was assigned. For example, if you want to add an event destination to a policy that was assigned using policy set, you can edit it in the policy set only. This also applies to group assignments.

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 to assets or asset groups.

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

Exporting and Importing Change Guardian Policies

Change Guardian allows you to export a policy to a `.xml` file. You can import that policy as a new policy. You can also modify an imported policy to create a new policy with a similar definition. You can export one policy at a time, however, you can import multiple policies at a time.

To export a policy:

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

To import a policy:

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

Assigning Event Destinations to Change Guardian Policies

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

To assign event destinations to a policy:

1. In Policy Editor, click **Change Guardian > Policy Assignment**.
2. Select an asset or asset group, and click **Assign Policies**.
3. Select a policy set or policy, and click **Advanced**.
4. Select one or more event destinations to assign to the specified policy or policy set.

For information about creating event destinations, see "Creating Event Destinations" on page 102.

Scheduling Change Guardian Policy Monitoring

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

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.

Policy Reports

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

Use the Policy Editor console to access administrative reports. The available report options are as follows:

- License Utilization
- Assigned Policies by Asset
- Asset Monitoring Failures
- Assets by Assigned Policies
- Managed Assets
- Policies not Assigned

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

For information about creating reports from the web console, see "Policy Details" in the *Change Guardian User Guide*. These reports can be emailed to other users for auditing or administration purposes.

For information about configuring SMTP, see "Changing Default Email Host Settings" on page 41.

7 Managing Events

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

- "Configuring Event Destinations" on page 101
- "Configuring Event Routing Rules" on page 103
- "Forwarding Events for Long-Term Retention" on page 105
- "Viewing Events" on page 105

Configuring Event Destinations

An event destination is where Change Guardian sends incoming events for a particular policy. You can view information about access and changes to critical files, systems, and applications. It is also where you deploy alert rules to notify you of those changes.

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

You can create and assign additional event destinations to meet your environment and regulatory needs. You can also change the default event destination. If you set another event destination as the default, all new policies automatically use the new default location. Existing policies continue to use their previously assigned event destinations. To change the event destinations for existing policies, see "Assigning Event Destinations" on page 103.

If your environment has multiple event destinations, and the default event destination is FIPS-enabled, some additional configuration steps are required. For more information, see "Configuring Event Destinations to Generate Alerts" on page 110.

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

Following sections provide information about creating event destinations.

- "Creating Event Destinations" on page 102
- "Assigning Event Destinations" on page 103

Creating Event Destinations

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

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

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

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

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

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

To create an event destination:

1. In Policy Editor, select **Settings > Event Destinations**
2. Click **Add**.
3. Specify a unique name for the event destination.
4. Specify one of the event destination models.
5. Provide system information of the server where you want to send events.

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

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

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

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

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

7. Click **OK**.

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

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

Assigning Event Destinations

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

To assign event destinations to a policy:

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

Configuring Event Routing Rules

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

Following sections provide information about configuring event routing rules.

- "Creating Event Routing Rules" on page 103
- "Ordering Event Routing Rules" on page 104
- "Activating or Deactivating an Event Routing Rule" on page 105

Creating Event Routing Rules

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

To create an event routing rule:

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

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

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

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

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

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

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

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

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

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

Select the email configuration that you already created using Policy Editor. For more information see Chapter 9, “Configuring Email Notifications,” on page 113.

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

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

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

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

Ordering Event Routing Rules

When there is more than one event routing rule, the event routing rules can be reordered by dragging them to a new 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 Administration Console, click **Routing** in the toolbar.

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

Existing event routing rules appear on the page.

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

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

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

Activating or Deactivating an Event Routing Rule

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

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

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

Existing event routing rules appear on the page.

2 To activate the event routing rule, select the check box next to each event routing rule in the **Enabled** column.

If the event routing rule is activated, a success message is displayed.

3 To deactivate the event routing rule, select the check box next to each event routing rule in the **Enabled** column.

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

Forwarding Events for Long-Term Retention

Change Guardian stores raw data and compressed event data on the local file system. You can configure Change Guardian to store the data in a networked location for long-term storage.

The data files are deleted from the local and networked storage locations on a configured schedule. Raw data retention is governed by a single raw data retention policy. Data retention is governed by a set of event data retention policies, which the Change Guardian administrator configures. By default, Change Guardian retains event data for 30 days.

Change Guardian uses the same data storage and retention policy technology as Sentinel. For more information, see "Configuring Data Storage" in the *Sentinel Administration Guide*.

Viewing Events

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

8 Configuring Alerts

Everything that happens in your environment creates an event. Most events are everyday occurrences and do not require any action on your part. A set of similar or comparable events in a given period, however, might indicate a potential threat. Alerts notify you of what is most important for you to look at. Alerts can relate to threats to IT resources or performance thresholds, such as system memory full or IT resources not responding.

This chapter provides the following information:

- "Understanding Alerts" on page 107
- "Managing Alerts" on page 107
- "Creating and Managing Alert Rules" on page 108
- "Creating and Managing Alerts Routing Rules" on page 110
- "Analyzing Alerts" on page 111
- "Configuring Alert Retention Policies" on page 111

Understanding Alerts

Change Guardian automatically associates the relevant events and identities with the alert to help you determine the root cause of a potential threat. For example, a change to the Windows file system or multiple failed logins within a specified time frame. Change Guardian uses alert rules to help you take appropriate actions to mitigate any problems. To receive instant notification about such potential threats, you can configure alert rules to create alerts.

Managing Alerts

As you monitor alerts, you can assign alerts to different users and roles, track the alert from origination to resolution, and annotate the alert rule by adding information to the knowledge base.

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

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

Creating and Managing Alert Rules

The following provides an overview of creating and monitoring alerts:

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

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

   As Change Guardian detects subsequent instances of the same alert, the product associates the trigger events to the existing alert to avoid duplication of alerts.

2. View and monitor alerts in the Administration Console.

   As you monitor alerts, you can assign alerts to different users and roles, track the alert from origination to resolution, and annotate the alert rule by adding information to the knowledge base.

3. Configure alert retention policies to specify when to automatically close and delete the alerts from Change Guardian.

- "Creating Alert Rules" on page 108
- "Redeploying Alert Rules" on page 110
- "Configuring Event Destinations to Generate Alerts" on page 110

Creating Alert Rules

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

Configure alert rules to create alerts when a matching event occurs. An alert contains almost the same information as the related event and also includes additional information specific to the alert, such as owner, state, and priority.

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

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

To create an alert rule:

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

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

- The policy or policies that you want to be alerted on.

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

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

  For example to select every policy name with DNS in the title, the alert rule creates alerts for all policies that contain DNS in the policy name, such as `DNS Configuration`.

- Whether you want to be alerted on severity and severity range.
- The event name or event names that you want to be alerted on.

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

  Following are a few categories for event names:

  - Active Directory
  - Configuration
  - File Systems
  - Group
  - Group Policy
  - Processes
  - User Accounts
  - Windows Specifics

- The event field or event fields that you want to be alerted on.
- Whether you want to be alerted on managed or unmanaged users.
- Whether you want to be alerted on event outcome.
- Whether you want to be alerted on IP address and its subnet.
- Alert criteria that further define the specific circumstances under which the alert rule creates an alert for the specified policies:

  - Generate an alert when an event occurs a specified number of times in a specified time frame.
  - Group alerts according to the specified event attributes.

- The event destinations to which you want to deploy the alert rule. By default, all available event destinations are selected.

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

Redeploying Alert Rules

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

If you make changes to the alert rule, such as modifying its alert criteria or adding information to the knowledge base and save, the alert rule is also redeployed automatically, to the given event destination. You can also redeploy the alert rule manually. Redeploying an alert rule ensures the event destination has the most recent version of the alert rule. For more information about the alert knowledge base, see the "Viewing and Triaging Alerts in Alert Views" in the *Change Guardian User Guide*.

Configuring Event Destinations to Generate Alerts

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

To ensure all event destinations receive alerts:

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

   `file: /etc/opt/novell/sentinel/config/sentinel.cer`
2. Change the credentials as follows:
   - `# chown novell:novell /path to certificate`
   - `# chmod 644 /path to certificate`
3. At the command prompt and go to `/opt/novell/sentinel/bin`.
4. Run the following command for all alternate event destinations:

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

Creating and Managing Alerts Routing Rules

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

- "Creating an Alert Routing Rule" on page 110
- "Ordering Alert Routing Rules" on page 111

Creating an Alert Routing Rule

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

To create an alert routing rule to filter the alerts:

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

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

Ordering Alert Routing Rules

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

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

Analyzing Alerts

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

Configuring Alert Retention Policies

You can configure the alert retention policies to set the duration to automatically close and delete the alerts from Change Guardian.

To configure the alert retention policy:

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

9 Configuring Email Notifications

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

- Use the Policy Editor to:
  - Add each email server to Change Guardian
  - Create one or more notification groups for each email server
- Use the Administration Console to assign email alerts to specified events. For more information, see "Creating Rules to Send Emails" on page 115.

This chapter provides the following information:

- "Configuring Email Servers" on page 113
- "Creating and Configuring Notification Groups" on page 114
- "Creating Rules to Send Emails" on page 115

Configuring Email Servers

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

Configure Email Servers to Change Guardian in FIPS Mode

1. Export the certificate from the respective SMTP server site.
2. Browse to the Sentinel bin directory. The default location is `/opt/novell/sentinel/bin`.
3. Import the certificate:

   ```
   convert_to_fips -i <certificate_path>
   ```
4. Restart the Change Guardian server using the following command:

   ```
   rcsentinel restart
   ```
5. Add new email configuration with STARTTLS protocol using Policy Editor.
6. Create routing rules in Administration Console.

Configure Email Servers to Change Guardian in Non-FIPS Mode

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

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

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

3 Restart the Change Guardian server:

```
rcsentinel restart
```

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

5 Create routing rules in Administration Console.

Adding Email Servers to Change Guardian

1 In the Policy Editor, select **Settings > Email Configuration**.

2 Under **Email Servers**, click **Add**.

3 Specify the name and description of the email server you want to add.

4 Specify values for the following fields:

- **SMTP Host:** The fully qualified domain name of the email server computer.
- **SMTP Port:** The remote SMTP port to use when communicating with the email server.
- **Secure:** Specifies whether the connection to the SMTP computer must be a secure connection. If **Yes**, specify the protocol type. If you select **No**, the **SMTP Port** will be set to **25** by default.
- **From**: The return email address appearing on each email alert for this email server.
- **Authentication Required:** Specifies whether the email server requires SMTP authentication to send email. If **Yes**, specify the following:
  - **User Name:** The user name to use when connecting to the SMTP server.
  - **Password:** The password corresponding to the specified SMTP user name.
- **Protocol:** Specifies which protocol can be used for the email communication. You can select **SSL** or **STARTTLS**.

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

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

Creating and Configuring Notification Groups

For each email server you add to Change Guardian, you must create one or more notification groups specific to that email server. A notification group specifies one or more recipients of the email alerts and contains change event information. When you assign email alerts to events in the Administration Console, you can choose from the notification groups available for that email server. For more information, see "Creating Rules to Send Emails" on page 115.

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.

Creating Rules to Send Emails

To send email messages from within the Administration Console, you must create an event routing rule and you must have an email server configured for the web console computer. If you do not have an email server configured, no notification groups appear as available actions for the event routing rule.

To assign email alerts to an event:

1. Log in to the Administration Console.
2. Click **Routing**, and then click **Create**.
3. Specify the relevant information for event routing.
4. Click **OK**.

NOTE: You can assign more than one email alert to a specific event by assigning more than one action to the event routing rule. Ensure that you set correct filters to avoid unnecessary flow of emails.

---

10 Configuring Data Federation

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

- "Overview" on page 117
- "Configuring an Authorized Requestor for Data Federation" on page 118
- "FIPS in Data Federation" on page 121
- "Viewing Search Activities" on page 122
- "Modifying the Data Source Server Details" on page 122
- "Troubleshooting" on page 123

Overview

When data federation is enabled, you can perform a search or run a report on one server and have it automatically run a search or report across the selected remote servers. The server on which the search is initiated is referred to as the authorized requestor, and the remote servers are referred to as the data sources or data source servers.

When you run a search or report on the authorized requestor, the following happens:

- Search queries are sent to each selected data source server
- Data source server authenticates the authorized requestor server
- Event or alert data is returned to the authorized requestor, where it is merged, sorted, and rolled up for presentation
- The search status for each data source server is displayed.

  Search results contain information about data source servers from which they originated.

Configuring an Authorized Requestor for Data Federation

You must first enable data federation on the authorized requestor server and then add data source servers to the authorized requestor server. You can add data source servers in the following ways:

- If you know the administrator username and password for the data source server, add the data source server directly from the authorized requestor.
- If you do not know the administrator username and password for a data source server, set up the authorized requestor with an opt-in password and share it with the source server. The administrator can use the opt-in password to add the data source servers to the authorized requestor.

- "Enabling Data Federation" on page 118
- "Using the Administrator Credentials to Add a Data Source Server" on page 118
- "Using the Opt-in Password to Add a Data Source Server" on page 119

Enabling Data Federation

To enable:

1. Create a role with **Proxy for Authorized Data Requestors** permission.

   For more information about configuring users and roles, see Configuring Roles and Users.
2. Log in as an administrator from Change Guardian Administration Console.
3. Click **Integration > Change Guardian**.
4. In the **Data Sources** section, select **Local server and other data sources**.
5. Do one of the following to add data source servers to your authorized requestor:
   - If you are the administrator of the authorized requestor and you know the administrator username and password for the data source server, continue with "Using the Administrator Credentials to Add a Data Source Server" on page 118.
   - If you are the administrator of the authorized requestor and you do not know the administrator user name and password on the data source server, continue with "Using the Opt-in Password to Add a Data Source Server" on page 119.

Using the Administrator Credentials to Add a Data Source Server

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

IMPORTANT: Ensure that the data source server that you add is able to communicate with the authorized requestor through TCP/IP. Use a ping command to ensure that the IP address or hostname of the data source server is accessible through firewalls or NATs. If there is a communication failure, an error is displayed in the extended status page. For more information, see "Managing Search Results" in the *Change Guardian User Guide*.

To add a data source server:

1. Complete the steps in "Enabling Data Federation" on page 118.
2. Click the **Add a data source** link.
3. Specify the following information:

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

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

   User Name: Name of a user with administrator privileges.

   Password: Password associated with the username.
4. Click **Login**, then click **Accept** after verifying that the certificate information is correct.
5. Specify the following information to configure the data source server:

   Name: Specify a descriptive name to identify the data source server.

   Search Proxy Role: Select a search proxy role that you want to assign to the authorized requestor. This permission is required for the data source server to accept and process incoming search requests from the authorized requestor server.

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

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

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

You can now search events, view event reports, and view alerts from the data source server. For more information, see Searching for Events, Running Federated Reports, and Viewing Federated Alerts respectively in the *Change Guardian User Guide*.

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

In organizations where administrative control of Change Guardian servers is decentralized, sharing administrator password might lead to violation of the security policy. If you do not have the administrator password for the data source server, Change Guardian allows you to set an opt-in password in the authorized requestor server, then provide the opt-in password to the data source server administrators to allow them to opt in to the authorized requestor server.

During the opt-in process, the authorized requestor and the data source server exchange the appropriate password, which allows the data source server to authenticate the search requests from the authorized requestor.

When a data source server opts in to the authorized requestor, a message is sent to the authorized requestor server requesting to be added to the list of data source servers. The authorized requestor requires an opt-in password to verify that the opt-in request has originated from a valid data source server. The request authorizes the authorized requestor to access data on the data source server.

- "Setting the Opt-In Password" on page 120
- "Allowing Access to an Authorized Requestor Server" on page 120

Setting the Opt-In Password

To set the password:

1. Complete the steps in "Enabling Data Federation" on page 118.
2. Click **Integration > Change Guardian**.
3. In the **Data Sources** section, select **Local server and other data sources**.
4. Click **Set Opt-in Password**.
5. Specify the opt-in password, then click **Set Password**.
6. Continue with "Allowing Access to an Authorized Requestor Server" on page 120 to add the data source server to the authorized requestor.

Allowing Access to an Authorized Requestor Server

To allow access:

1. Log in to the data source server as an administrator.
2. Click **Integration > Change Guardian**.
3. From the **Authorized Requestors** section, check the **Allow authorized requestors to access data from your server** box.
4. Click the **Add** link.
5. Specify the following information:

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

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

   Opt-in Password: The opt-in password that you configured on the authorized requestor. You must obtain this password from the administrator of the authorized requestor.
6. Click **OK**.
7. Verify the certificate information, then click **Accept**.
8. Specify the following information to configure the data source server:

   Name : A descriptive name to identify the authorized requestor server.

   Search Proxy Role : A proxy role to assign to the authorized requestor.

This permission is required for the data source server to accept and process incoming search requests from the authorized requestor server. When the authorized requestor makes search requests to the data source server, the security filter of the proxy role is used. Only those events that pass the security filter of the proxy role are returned to the authorized requestor server. Only roles that have the Proxy for Authorized Requestors permission are listed.

9 Click **OK**.

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

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

FIPS in Data Federation

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

To add certificates:

1 Log in to the distributed search source computer.

2 Browse to the following certificate directory:

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

3 Copy the source certificate (`sentinel.cer`) to a temporary location on the requestor computer.

4 Import the source certificate into the FIPS keystore of the requestor server.

For more information about importing the certificate, see Importing certificates into the FIPS keystore database.

5 Log in to the distributed search requestor computer.

6 Browse to the following certificate directory:

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

7 Copy the requestor certificate (`sentinel.cer`) to a temporary location on the source computer.

8 Import the requestor system certificate into the FIPS keystore of the source server.

For more information about importing the certificate, see Importing certificates into the FIPS keystore database.

Importing Certificates into the FIPS Keystore Database

To import certificates:

1 Copy the certificate file to any temporary location on the Change Guardian server or remote Collector Manager.

2 Change the ownership of the certificate to `novell` user:

```
chown novell:novell /<path to certificate>
```

3 Change the permission of the certificate:

`chmod 644 /<path to certificate>`

4 Switch to `novell` user.

5 Browse to the Sentinel bin directory.

The default location is `/opt/novell/sentinel/bin`.

6 Import the certificate into the FIPS keystore database, and then follow the on-screen instructions:

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

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

Viewing Search Activities

You can view the type and frequency of search activities run on the data source server by the authorized requestor server. Based on the search activity, you might want to assign a more or less restrictive proxy role or even disable access to the data source server.

You can also refine the search activity query. For example, you can change the date range to see the queries performed today, yesterday, or in the last hour. You can also see the queries that were made by particular users on the authorized requestor.

To view search:

1 Log in to the data source server as an administrator.

2 Click **Integration > Change Guardian**.

3 From the **Authorized Requestors** section, click the **Search Activities** link for the authorized requestor server for which you want to view the search activities.

A list of the audit events that are retrieved from all the distributed search requests that a data source server has received from an authorized requestor are displayed.

Modifying the Data Source Server Details

You can modify the name of the data source server and the port number.

To modify the details:

1 From the Administration Console log in as an administrator.

2 Click **Integration > Change Guardian**

3 In the **Data Sources** section, click the **Edit** link for the data source server that you want to modify.

4 Make the necessary modifications.

5 (Optional) To change the proxy role on the data source server, complete the following steps:

5a Click **View/Change**.

5b Log in to the data source server.

5c Select a proxy role, then click **OK**.

6 Click **Save**.

Troubleshooting

This section lists the most common issues and the probable causes for these issues.

- "Permission Denied" on page 123
- "Connection Down" on page 123
- "Unable to View Raw Data" on page 124
- "Problems While Adding Data Source" on page 124
- "Some Events Are Only Visible from the Local System" on page 124
- "Cannot Run Reports on the Data Source Servers" on page 124
- "Different Users Get Different Results" on page 124
- "Cannot Set the Administrator Role as the Search Proxy Role" on page 124
- "Error Logs" on page 124

Permission Denied

After doing a distributed search, check the extended status page to view the search status. If the search is not successful, check the following possible causes:

- The data source server administrator might have disabled data federation on the data source server. To enable data federation on the data source server, see Step 3 in "Allowing Access to an Authorized Requestor Server" on page 120.
- The data source server administrator might have disabled the authorized requestor server for data federation. Ensure that the authorized requestor server is enabled in the data source server. For more information, see "Allowing Access to an Authorized Requestor Server" on page 120.
- The role that you used to connect might not have the `Search Data Targets` permission.

Connection Down

- Network issues in your organization.
- Change Guardian servers or Change Guardian services might be down.
- Connection might have time-out.
- The IP address or the port number of the data source server has changed, but the authorized requestor configuration might not be updated.

Unable to View Raw Data

The Proxy group that is assigned to the authorized requestor might not have the `view all events` permission to view the raw data.

Problems While Adding Data Source

The authorized requestor server and the data source server might not be communicating with each other. Ensure that the firewall and NAT are set up properly to allow communication in both directions. Ping both ways to test.

Some Events Are Only Visible from the Local System

You might not be able to view the events from the data source servers for one of the following reasons:

- The trial license might have expired. You must purchase an enterprise license to reactivate this feature to view events from the data source servers.
- The user who has logged in to the authorized requestor has one set of permissions on the local data, such as view all data, view system events, security filter settings, and the search proxy group has another set of permissions, possibly more restrictive. Therefore, certain types of data, such as raw data, system events, and PCI events, might be returned only from the local system and not the data source server.

Cannot Run Reports on the Data Source Servers

The trial license might have expired. You must purchase an enterprise license to reactivate this feature to run reports from the data source servers.

Different Users Get Different Results

Different users might have different security filters or other permissions and therefore get different results from a distributed search.

Cannot Set the Administrator Role as the Search Proxy Role

This is by design, for security reasons. Because the data viewing rights for the administrator are unrestricted, it is not desirable to allow the administrator role to be the search proxy role.

Error Logs

You can also determine the cause of a search failure by examining the log file on the authorized requestor server. The default location for the log file is `/var/opt/novell/Change Guardian/log`. For example, you might see one of the following messages:

```
Invalid console host name 10.0.0.1
```

```
Error sending target request to console host 10.0.0.1
```

```
Error getting certificate for console host 10.0.0.1

Authentication credentials in request to opt-in to console 10.0.0.2 were
rejected

Request to opt-in to console 10.0.0.2 was not authorized

Error sending target request to console host 10.0.0.1
```

11 Configuring Integrations with Other Software

This section provides information about integrating Change Guardian with the Security Information and Event Management (SIEM) solutions to forward event to enhance event analysis, use Identity Management Systems to get user details, and track Active Directory using Directory and Resource Administrator (DRA) as events.

This chapter provides the following information:

- "Integration with SIEM Solutions" on page 127
- "Integrating with Identity Management Solutions" on page 127
- "Integration with Directory Resource Administrator" on page 130

Integration with SIEM Solutions

Change Guardian and the SIEM solution products, such as Micro Focus Sentinel Enterprise, Splunk Enterprise Security, and ArcSight Enterprise Security Manager are security monitoring solutions. Change Guardian provides focused security for change details and privilege user monitoring, and can forward these specialized change monitoring details to other SIEM solutions for consolidated monitoring, correlations and analysis.

SIEM Product Name	Event Forwarding Mechanism
Sentinel	REST Dispatcher or Syslog Dispatcher
Splunk Enterprise Security	Syslog Dispatcher
ArcSight Enterprise Security Manager	Syslog Dispatcher

In Sentinel you can analyze the change events forwarded by Change Guardian, while the other SIEM solution products use Change Guardian to analyze the data.

To configure event forwarding to other SIEM solution products, see "Configuring Event Destinations" on page 101.

Integrating with Identity Management Solutions

Change Guardian provides an integration framework for AD or IDM to track identities of each user account and what events those identities have performed.

This integration provides functionality on several levels:

- The People Browser provides the ability to look up the following information about a user:
  - Contact information

- Accounts associated with that user
- Most recent authentication events
- Most recent access events
- Most recent permissions changes

- Reports and Correlation rules provide an integrated view of a user's true identity, even across multiple systems on which the user has separate accounts. For example, accounts like `COMPANY\testuser; > cn=testuser,ou=engineering,o=company`, and `TUser@company.com` can be mapped to the actual person who owns the accounts.

By displaying information about the people initiating a given action or people affected by an action, incident response times are improved and behavior-based analysis is enabled.

NOTE: Only administrators can integrate Change Guardian with identity management systems.

Integrating with Active Directory

Change Guardian only provides initiator's user name and the ObjectSID of an event during auditing activities. However, more information is essential to detect and assess risks.

The benefits of Change Guardian integration with AD are as follows:

- Permits the Change Guardian server to retrieve user information from AD and map with associated incoming events.
- Helps map user profiles with attributes in the web console.

These allow you to enrich available information and so better detect and assess risks. Some additional features also include:

- Receive delta values from AD.
- Support for adding additional attributes.
- Support for mapping custom attributes.
- Synchronize users from multiple user containers concurrently.
- Synchronize deleted users.

Synchronizing Active Directory User Accounts

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

- "Adding a User Container" on page 129
- "Mapping User Profile Fields" on page 129

Using the Administration Console, you add one or more user containers and the user attributes that you want to synchronize.

To view and manage synchronized Active Directory accounts:

1. In the Administration Console, click **Integration**.
2. Click **AD Accounts**.

Adding a User Container

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

To add a user container to Change Guardian:

1. In the Administration Console, click **Integration > AD Accounts > Add User Container**.
2. Provide the appropriate information for the user container you want to synchronize.

Mapping User Profile Fields

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

To modify user profile mapping, in the Administration Console, click **Integration**> **AD Accounts**> **User Profile Mapping**.

Integration with Identity Manager

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

To view user identity details:

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

For more information about integrating identity information with Change Guardian events, see "Integrating Identity Information" in the *"Sentinel Administration Guide"*.

Searching and Viewing Identity Information

To search and view identity information, see Searching and Viewing User Identities in the *"Change Guardian User Guide".*

Integration with Directory Resource Administrator

Change Guardian provides enhanced user monitoring in conjunction with DRA. It provides solution to control, manage and monitor the Active Directory environments.

Change Guardian server captures the unmanaged changes on DRA and displays the *actual* user name (end-user who logged in to DRA) in the event list on the Administration Console. As an auditor you can monitor the AD audit logs or events from DRA, and view the corresponding actual user name on the Change Guardian event list.

Prerequisites:

Ensure that you have completed the following:

- Install DRA
- Install Change Guardian

Setting Up Change Guardian

To set up Change Guardian to recieve DRA events, perform the following steps:

- Installing Change Guardian Agent for Windows
- Adding License Keys
- Configuring AD
- Creating an AD Policy
- Assigning Policies

Setting Up DRA

To set up DRA, perform the following steps:

- To “manage AD domains”, see the *Directory and Resource Administrator Administrator Guide*
- Enabling Event Stamping
- Configuring Unified Change History

Enabling Event Stamping in DRA

Event stamping allows Change Guardian to receive the DRA user details.

When AD Domain Services auditing is enabled, DRA events are logged as having been generated by either the DRA Service account or the Domain Access account if one is configured. Event Stamping takes this feature one step further by generating an additional AD DS event that identifies the assistant administrator who performed the operation.

For these events to be generated you must configure AD DS auditing and enable Event Stamping on the DRA Administration Server. When Event Stamping is enabled, you will be able to view the changes that assistant administrators make in Change Guardian Event reports.

- To configure AD DS auditing, see the Microsoft reference *AD DS Auditing Step-by-Step Guide*.

- To configure Change Guardian integration, see "Configuring Unified Change History Servers" on page 132.
- To enable Event Stamping, open the Delegation and Configuration console as DRA Administrator, and do the following:
  1. Navigate to **Configuration Management** > **Update Administration Server Options** > **Event Stamping**.
  2. Select an object type, and click **Update**.
  3. Select an attribute to use for Event Stamping for that object type.

     DRA currently supports Event Stamping for users, groups, contacts, computers, and organizational units.

     DRA also requires that the attributes exist in the AD schema for each of your managed domains. You should be aware of this if you add managed domains after configuring Event Stamping. If you were to add a managed domain that does not contain a selected attribute, operations from that domain would not be audited with the Event Stamping data.

     DRA will be modifying these attributes so you should select attributes that are not used by DRA or any other application in your environment.

Configuring Unified Change History in DRA

The Unified Change History Server feature enables you to generate reports for changes made outside of DRA.

Delegating the Unified Change History Server Configuration Powers

To manage Unified Change History Server, assign the Unified Change History Server Administration role or the applicable powers below to assistant administrators:

- Delete Unified Change History Server Configuration
- Set Unified Change History Configuration Information
- View Unified Change History Configuration Information

To delegate Unified Change History Server powers:

1. Click **Powers** in the Delegation Management node, and use the search objects feature to find and select the UCH powers that you want.
2. Right-click one of the selected UCH powers and select **Delegate Roles and Powers**.
3. Search for the specific user, group, or assistant administrator group that you want to delegate powers to.
4. Use the **Object Selector** to find and add the objects that you want, and then click **Roles and Powers** in the **Wizard**.
5. Click **ActiveViews**, and use the **Object Selector** to find and add the ActiveViews that you want.
6. Click **Next** and then **Finish** to complete the delegation process.

Configuring Unified Change History Servers

To configure Unified Change History Servers:

1. Log in to the Delegation and Configuration Console.
2. Expand **Configuration Management** > **Integration Servers**.
3. Right-click **Unified Change History**, and select **New Unified Change History Server**.
4. Specify the UCH server name or IP address, port number, server type, and access account details in the Unified Change History configuration.
5. Test the server connection and click **Finish** to save the configuration.
6. Add additional servers as required.

Viewing DRA Events in Change Guardian

To view DRA events, see Change Guardian dashboard. The Change Guardian event details display the application as DRA.

Viewing Change Guardian Reports in DRA

To view the Unified Change History reports on AD objects from Change Guardian, see “Utilizing Unified Change History” in the *Directory and Resource Administrator User Guide*.

Issues Coexisting with Change Guardian

Change Guardian events do not display the actual DRA user name in the following scenarios:

- When you define the computer account enabled or disabled, user account unlock policies.
- When you make any modifications in the Group scope or Group Type.
- When you make changes to the remote access permission in Dial In tab in DRA, two modification events are populated.The event shows User-Parameters in the delta.
- When you make changes in Azure AD and Exchange using DRA.
- When you make changes in the following tabs in DRA:
  - Account tab
  - Password tab
  - Member of tab
  - Terminal Services tab
  - Dial in tab
  - Call back tab

12 Backing Up and Restoring Data

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

NOTE: To ensure compatibility you must restore backed up data to the same version of Change Guardian, use the same computer (IP address and Hostname match) you used to create the backup and ensure that the install configuration or custom path (if any) and FIPS configuration also match the original.

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

- **System Failure**: If system fails, you must first reinstall Change Guardian and then use the `cgbackup_util.sh` script with the restore parameter to restore the most recent data that you backed up.
- **Data Loss**: If data is lost, use the `cgbackup_util.sh` script with the restore parameter to restore the most recent data that you backed up.

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

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

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

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

This chapter provides the following information:

- "Parameters for the Backup and Restore Utility Script" on page 134
- "Running the Backup and Restore Utility Script" on page 136
- "Restoring Data" on page 138

Parameters for the Backup and Restore Utility Script

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

Table 12-1 *Backup and Restore Script Parameters*

Parameters	Description
`-m backup`	Backs up the specified data.
`-m restore`	Restores the specified data. The restore mode of the script is interactive and allows you to specify the data to restore from the backup file. The restore parameter can be used in the following scenarios: ◆ **System Failure:** In the event of a system failure, you must first reinstall Change Guardian and then use the `cgbackup_util.sh` script with the restore parameter to restore the most recent data that backed up. ◆ **Data Loss:** In the event of data loss, use the `cgbackup_util.sh` script with the restore parameter to restore the most recent data that you had backed up. You must restart the Change Guardian server after you restore any data because the script might make several modifications to the database.
`-m info`	Displays information for the specified backup file.
`-m simple_event_backup`	Backs up events located in a specified directory.
`-m simple_event_restore`	Restores events into a specified directory.
`-c`	Backs up the configuration data, Policy Editor settings, policies created, and policies assigned.
`-e`	Backs up the event data. All event partitions are backed up except the current online partition. If the backup is being performed with the Change Guardian server shut down, the current online partition is also included in the backup. It backs up event data from all the directories and subdirectories.

Parameters	Description
-dN	Backs up the event data for the specified number of days. The -dN option backs up the primary storage event data stored for the last N days. Based on the current data retention policy settings, many days of events might be stored on the system. Backing up all of the event data might not always be necessary and might not be desirable. This option allows you to specify how many days to include when backing up the event data. For example, -d7 includes only the event data from the last week in the backup. -d0 just includes the data for the current day. -d1 includes the data from the current day and previous day. -d2 includes the data from the current day and two days ago. Online backups (that is, backups performed while the system is running) only back up the closed event partitions, which means partitions one day old or older. For online backups, a value of -d1 is the appropriate specification for the number of days.
-u	Specifies the user name to use when backing up the event associations data. If the user name is not specified, admin is the default value. This parameter is required only when backing up the event associations data.
-p	Specifies the user password when backing up the event associations data. This parameter is required only when backing up the event associations data.
-x	Specifies a file name that contains the user password when backing up the event associations data. This is an alternative to the -p parameter. This parameter is required only when backing up the event associations data.
-f	Specifies the location and name of the backup file.
-l	Includes the log files in the backup. By default, the log files are not backed up unless you specify this option.
-r	Includes the runtime data in the backup. To back up runtime data, you must shut down the Change Guardian server because data is dynamic. This parameter must be used in combination with the -s option (described below). If -s is not specified, this parameter is ignored.
-b	Backs up the NetFlow data collections and not the entire MongoDB database. The following baseline data is backed up: ◆ configs ◆ anomalydefs ◆ baselines ◆ baselines.ID.URN ◆ paths.UUID.URN ◆ anomalydeployment
-A	Backs up alerts and the events that triggered the alert.
-i	Backs up the entire MongoDB database, NetFlow data collections, and alerts.

Parameters	Description
-s	Shuts down the Change Guardian server before performing the backup. Shutting down the server is necessary to back up certain dynamic data, such as the runtime data and current primary storage partitions. By default, the server does not shut down before the backup. If you use this option, the server restarts automatically after the backup is complete.
-w	Backs up the raw event data.
-z	Specifies the location of the event data directory, such as where the event data is collected during a simple_event_backup and where the event data is placed during a simple_event_restore. Only available with the simple_event_backup and simple_event_restore options.

Running the Backup and Restore Utility Script

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

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

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

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

For more information about different parameters, see Table 12-1. The following table lists examples of how to specify the parameters:

Syntax	Action
cgbackup_util.sh -m backup -c -e -i -l -r -w -s -u admin -x <*mypassword.txt*> -f /var/opt/novell/sentinel/data/<*my_full_backup*>.tar.gz	Shuts down the Change Guardian server and performs a full system backup.
cgbackup_util.sh -m backup -c -e -i -l -w -u admin -x <*mypassword.txt*> -f /var/opt/novell/sentinel/data/<*my_weekly_backup*>.tar.gz	Performs an online backup without shutting down the server. This backup includes everything except online event data and dynamic runtime data.

Syntax	Action
`cgbackup_util.sh -m backup -b -c -e -d7 -u admin -x <mypassword.txt> -f /var/opt/novell/sentinel/data/<my_weekly_backup>.tar.gz`	Performs an online backup with event data from the last week. This backup includes configuration data and the event data for the last seven days. Event data older than seven days is not backed up because that data can be extracted selectively, if necessary, from an older backup.
`cgbackup_util.sh -m backup -c -f /var/opt/novell/sentinel/data/<my_full_backup>.tar.gz`	Performs a local backup of the configuration data. This is a minimal backup of the system without any event data.
`cgbackup_util.sh -m backup -e -f /var/opt/novell/sentinel/data/events_backup.tar.gz`	Performs a local backup of the event data. This is a minimal backup of the primary storage event data.
`cgbackup_util.sh -m backup -e -d5 -f /var/opt/novell/sentinel/data/events_5days_backup.tar.gz`	Performs a local backup of the event data from the last five days. This is a minimal backup of the primary storage event data from the last five days.
`cgbackup_util.sh -m info -f /var/opt/novell/sentinel/data/<my_full_backup>.tar.gz`	Displays the backup information for the specified backup file.
`cgbackup_util.sh -m simple_event_backup -e -z /opt/archives/archive_dir -f /opt/archives/archive_backup.tar.gz`	Performs a backup of event data on the computer where the secondary storage directory is located. If the `/opt/archives/archive_dir` is not located in the server, you might need to copy the `cgbackup_util.sh` script to the computer where the secondary storage is located and then run the `simple_event_backup` command from that computer. Alternatively, you can also use any third-party backup tool to back up the event directories on secondary storage.
`cgbackup_util.sh -m restore -f /var/opt/novell/sentinel/data/<my_full_backup>.tar.gz`	Restores the data from the specified filename. **NOTE:** To successfully restore the data from backup, ensure that the backup file ownership is set to user `novell` and group `novell`.

Syntax	Action
`cgbackup_util.sh -m simple_event_restore -z /opt/archives/archivedir -f /opt/archives/archive_backup.tar.gz`	Restores the secondary storage data.

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

4 Use the Data Restoration feature to restore the extracted partitions. For more information, see "Restoring Data" on page 138.

Restoring Data

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

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

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

- "Enabling Event Data for Restoration" on page 138
- "Viewing Event Data Available for Restoration" on page 139
- "Restoring Event Data" on page 139
- "Configuring Retention Period" on page 140

Enabling Event Data for Restoration

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

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

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

Viewing Event Data Available for Restoration

1. Log in to the Administration Console as a user in the administrator role.
2. Click **Storage** > **Configuration**.

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

   The Data Restoration table chronologically lists all the event data that can be restored. The table displays the date of the event data, the name of event directory, and the location. The **Location** column indicates whether the event directory was found in the primary storage directory of Change Guardian or in the configured secondary storage directory.
4. Continue with "Restoring Event Data Where UID and GID are not the Same on the Source and the Destination Server" on page 139 to restore the event data.

Restoring Event Data

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

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

   The selected events are moved to the **Restored Data** section. It might take approximately 30 seconds for the **Restored Data** section to reflect the restored event partitions.
3. (Optional) Click **Refresh** to search for more restorable data.
4. To configure the restored event data to expire according to data retention policy, continue with "Restoring Data" on page 138.

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

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

To unsquash and squash the file system:

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

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

   `cd /var/opt/novell/sentinel/data/archive_remote/<sentinel_server_UUID>/eventdata_archive/<partition_ID>`
4. Unsquash the `index.sqfs` file:

```
unsquashfs index.sqfs
```

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

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

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

6 Remove the index:

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

7 Switch to novell user:

```
su novell
```

8 Squash the `squashfs-root` folder:

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

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

Configuring Retention Period

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

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

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

13 Upgrading Change Guardian

This chapter provides information about the following sections:

- "Upgrade Checklist" on page 141
- "Prerequisite" on page 142
- "Upgrading a Traditional Installation" on page 142
- "Upgrading the Appliance Installation" on page 144
- "Upgrading Components" on page 147
- "Applying Updates to Change Guardian Components" on page 148
- "Adding Application License after Upgrade" on page 149
- "Post Upgrade Configuration" on page 149
- "Verifying the Upgrade" on page 150
- "Troubleshooting" on page 150

Upgrade Checklist

You can upgrade to Change Guardian 6.0 from Change Guardian 5.1 or later.

For information about appliance upgrade paths, see "Appliance Upgrading Paths" on page 153.

You must upgrade both the Change Guardian server and Policy Editor. The Change Guardian Agent for Windows is backward compatible.

Use the following checklist to upgrade your Change Guardian installation:

Table 13-1 *Upgrade Checklist*

	Tasks	See
❒	Ensure that the computers on which you install Change Guardian components meet the specified requirements. **NOTE:** Change Guardian is not supported if the operating system is in FIPS mode.	Supported Platforms on the System Requirements page.
❒	Understand the order for the upgrade before upgrading the operating system on the Change Guardian server,	"Upgrading the Appliance Installation" on page 144
❒	Review the SUSE Release Notes for known issues related to the supported operating system.	SUSE Release Notes
❒	Review the Change Guardian Release Notes to see the new functionalities and understand the known issues.	Release Notes

	Tasks	See
❒	Upgrade the Change Guardian server. **NOTE:** If the Change Guardian server is running on FIPS mode, enable TLS 1.1 after upgrading the Change Guardian server.	◆ "Upgrading a Traditional Installation" on page 142 ◆ "Upgrading the Appliance Installation" on page 144
❒	Upgrade the Change Guardian components.	◆ "Upgrading Components" on page 147 ◆ "Upgrading Change Guardian Agent for Windows" on page 148 ◆ Upgrading Security Agent for UNIX.

Prerequisite

Ensure that the latest patch of Microsoft Windows is running on the system on which the Change Guardian Agent for Windows is running.

Upgrading a Traditional Installation

Perform the installation in the following order:

1. Upgrading Change Guardian
2. Upgrading the Operating System

Upgrading Change Guardian

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

To upgrade the Change Guardian Server in a traditional installation:

1 Back up your information using the `cgbackup_util.sh` script.

For information about using the backup utility, see Chapter 12, "Backing Up and Restoring Data," on page 133.

2 Download the latest installer from the Micro Focus Patch Finder website.

You must be a registered user to download patches. If you have not registered, click **Register** to create a user account in the patch download site.

3 Copy the installer file to a directory that has 0755 permissions.

NOTE: Trying to upgrade from any directory within `/root` fails because certain upgrade commands run as non-root user. Such commands cannot run if the installer is in the `/root` directory.

4 Log in as `root` to the Change Guardian server you want to upgrade.

5 Extract install files from the tar file:

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

6 Change to the directory where the install file was extracted.

7 Start the upgrade:

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

8 (Conditional) If you want to upgrade from a custom path, specify the following command:

```
./install-changeguardian.sh --location=<custom_CG_directory_path>
```

NOTE: You can only upgrade from a custom path used for the original installation and the path must have 0755 permissions.

---

9 To proceed with a language of your choice, select the number next to the language.

10 If there are changes to the end user license agreement, read and accept the changes.

11 To select the desired migration option, enter option 1, 2, or 4.

WARNING: Ensure that you select the appropriate option because you cannot repeat this procedure after the upgrade is successful.

The data that was stored in MongoDB is retained as a backup.

12 (Conditional) If data migration is not successful, clean up data from PostgreSQL.

13 Specify `yes` to approve the upgrade.

The upgrade might take a few seconds to complete.

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

15 (Conditional) The data in MongoDB is redundant because Change Guardian 6.0 stores data only in PostgreSQL. To remove redundant data from MongoDB, clear the disk space:

```
./mongodb_cleanup.sh
```

16 Verify that you see the migrated content and that you are receiving new alerts by logging in to the Threat Response Dashboard.

17 Verify that you can connect to the Change Guardian web interface by accessing the following URL:

`https://IP_Address_Change_Guardian_server:8443`

Based on your security requirement, perform the post upgrade configurations.

Upgrading the Operating System

If the Change Guardian server is running a version of an operating system that is not certified, some features might not function as expected. Upgrade to a supported operating system for a seamless experience.

To upgrade the operating system:

1 Log in as `root` to the machine running Change Guardian.

2 Stop the Change Guardian services:

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

3 (Conditional) If Change Guardian was in FIPS mode before the operating system upgrade, upgrade the NSS database:

```
certutil -K -d sql:/etc/opt/novell/sentinel/3rdparty/nss -X
```

Follow the on-screen instructions to upgrade the NSS database.

Give full permissions to `novell` user for the following files in the `/etc/opt/novell/sentinel/3rdparty/nss` directory:

```
cert9.db
key4.db
pkcs11.txt
```

4 Upgrade the operating system.

5 (Conditional) If you use Mozilla Network Security Services (NSS) 3.29 or later, install the two dependent RPM files:

- `libfreebl3-hmac`
- `libsoftokn3-hmac`

6 (Conditional) For RHEL 7.x, check whether there are any errors in the RPM database:

```
rpm -qa --dbpath <install_location>/rpm | grep novell
```

Example: `# rpm -qa --dbpath /custom/rpm | grep novell`

- If there are any errors, fix the errors:

  ```
  rpm --rebuilddb --dbpath <install_location>/rpm
  ```

  For example: # rpm --rebuilddb --dbpath /custom/rpm

- Recheck that there are no errors:

  ```
  rpm -qa --dbpath <install_location>/rpm | grep novell
  ```

Upgrading the Appliance Installation

This section provides the following information:

- "Running the Appliance Configuration Utility" on page 144
- "Applying Updates" on page 145

Running the Appliance Configuration Utility

The appliance configuration utility migrates alerts data from MongoDB to PostgreSQL

To run the utility:

1 Download the migration file `changeguardian_appliance_configuration_utility_6000-01.tar.gz` from Change Guardian downloads page.

2 Log in to the server as `root`.

3 Extract the files to your local server:

```
tar -zxvf changeguardian_appliance_configuration_utility_6000-01.tar.gz
```

4 Change to the directory where the file was extracted.

5 Run the migration utility:

```
./cg6000_appliance_configuration.sh
```

6 To select the desired migration option, enter 1, 2, or 4.

7 (Conditional) If data migration is not successful, clean up data from PostgreSQL.

8 (Conditional) The data in MongoDB is redundant because Change Guardian 6.0 stores data only in PostgreSQL. To remove redundant data from MongoDB, clear the disk space:

```
./mongodb_cleanup.sh
```

WARNING: After you migrate data, you must upgrade Change Guardian before you start or restart Change Guardian.

Applying Updates

The following are the two methods in which you can apply updates:

- "Applying Updates By Using the Change Guardian Appliance Console" on page 145
- "Applying Updates Using Zypper" on page 145
- "Performing Offline Updates" on page 146

Applying Updates By Using the Change Guardian Appliance Console

To apply updates:

1 Register to the Change Guardian appliance update channel.

2 Get the Change Guardian and the operating system updates from the appliance update channel.

3 Log in to the Change Guardian Appliance Console as `vaadmin` or `root` user using the following URL: `https://IP_Address_Change_Guardian_server:9443`.

4 Click **Online Update**.

5 Select **Needed Patches** from the drop-down list and click **Update Now**.

6 Select **Needed Patches** from the drop-down list to ensure that there are no pending updates.

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

8 Install the operating system package updates:

```
zypper up
```

Applying Updates Using Zypper

Zypper is a command-line package manager that allows you to perform an interactive upgrade of the Change Guardian appliance.

To update the appliance:

1. Register to the Change Guardian appliance update channel.
2. Get the Change Guardian and the operating system updates from the appliance update channel.
3. Log in to the Change Guardian server as `root`.
4. Check for available updates:

   ```
   zypper lp
   ```
5. Run the following command:

   ```
   zypper patch
   ```

   This checks the installed packages and resolves any file conflicts.
6. Rerun the command to install appliance updates:

   ```
   zypper patch
   ```
7. Install the operating system updates:

   ```
   zypper up
   ```
8. Restart the Change Guardian appliance:

   ```
   reboot
   ```

For more information about Zypper, see Zypper Cheat Sheet.

Performing Offline Updates

You can perform an update by using an offline ISO file under the following conditions:

- When there is no internet access and you are unable to register the appliance.
- When you prefer not to download the latest release available in the appliance download repository, but an earlier release. For more information, see Product Support Lifecycle.
- When the current version that you are running is incompatible with the latest version, download a version that is compatible and then upgrade it to the latest version. For more information, see Product Support Lifecycle.

While applying the patch, if you encounter registry/repository issues, clear the registry and repository entries in your system.

To clean up the registration and repository details on the appliance:

- Take a backup of the files before clearing the registry entries and create a backup directory. For example: `mkdir /etc/zypp/backup`
- Copy the following registry files to the backup directory. For example:
  - cp /etc/zypp/credentials.d /etc/zypp/backup
  - cp /etc/zypp/repos.d/* /etc/zypp/backup
  - cp /etc/zypp/services.d/* /etc/zypp/backup
- Delete the following registry files:

  ```
  rm -fr /etc/zypp/credentials.d
  ```

```
rm -fr /etc/zypp/repos.d/*
rm -fr /etc/zypp/services.d/*
```

For more information, contact Technical Support.

Applying the ISO Patch

Pre-requisites:

Download and run the utility `change_guardian_appliance_configuration_utility-<version>.tar.gz` from Change Guardian downloads page.

1. Download the patch to a directory. For example: `<directoryname>/change_guardian_offline_appliance-<version>.iso`
2. Create a directory for mounting the CD using a command. For example: `mkdir -p /opt/trial`
3. Mount the patch CD locally using a command. For example:

   ```
   mount <directoryname>/change_guardian_offline_appliance-<version>.iso /opt/trial
   ```
4. Add the product and operating system repositories. For example:

   ```
   zypper ar -c -t plaindir "/opt/trial/product-repo" "<product repository>"
   zypper ar -c -t plaindir "/opt/trial/osupdate-repo" "<operating system repository>"
   ```
5. (Optional) Confirm if the repos are added successfully using the command: `zypper repos`
6. Check if the patches are bundled in the patch CD using the command: `zypper lp`
7. Run command `zypper patch`. This checks the installed packages and resolves any file conflicts.
8. Rerun the command to install appliance updates: `zypper patch`
9. Install the operating system updates: `zypper up`
10. Clean up the repositories list using the following command:

    ```
    zypper rr "<product repository>"
    zypper rr "<operating system repository>"
    ```
11. Start Change Guardian services before reboot: rcsentinel start
12. After the update is complete, reboot the machine using the command: `reboot`

Upgrading Components

- "Upgrading Policy Editor" on page 148
- "Upgrading Change Guardian Agent for Windows" on page 148
- "Upgrading Security Agent for UNIX" on page 148

Upgrading Policy Editor

To upgrade Policy Editor, see "Installing Policy Editor" on page 31.

Upgrading Change Guardian Agent for Windows

You can upgrade Change Guardian Agent for Windows manually or by using Agent Manager. You can also roll back an update.

NOTE: The procedure for upgrading the Change Guardian Agent for Windows manually is the same as the procedure for installing them, except that you do not need to repeat the process of adding assets to Agent Manager. Do not rename the default `.msi` installer package. For more information, see "Manual Installation" on page 33.

To upgrade using Agent Manager:

1. From assets list, select the agent you want to upgrade.

   You can select multiple assets if Agent Manager uses the same credentials to connect to them.
2. Provide login credentials to connect to the assets and click **Next**.

   The account must be a local administrator account or a domain account in the Local Administrators group of the asset.
3. Click **Manage Installation > Upgrade**.
4. Select the agent.
5. Click **Start Upgrade**.

Upgrading Security Agent for UNIX

You can upgrade Security Agent for UNIX by using Agent Manager.

To upgrade Security Agent for UNIX:

1. From the assets list, select the asset where you want to upgrade the agent.

   If you select multiple computers, you must use the same credentials in all computers.
2. Click **Manage Installation > Upgrade**.
3. Select the agent.
4. Click **Start Upgrade**.

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, Security Agent for UNIX, or Policy Editor.

To apply the patch:

1. Download the patch from the Micro Focus Patch Finder.

2 Log in to Agent Manager.

3 Click **All Assets > Manage Installation > Upload Package**.

This uploads the package to the Change Guardian server.

4 To upgrade agents or download Policy Editor, log in to Agent Manager on the machine running the agent or Policy Editor.

5 (Conditional) To upgrade Policy Editor, click **All Assets > Manage Installation > Download Package**, and then begin upgrade.

For more information about upgrading, see Upgrade Policy Editor.

6 (Conditional) To upgrade agents, click **Manage Installation > Upgrade Agents**.

Adding Application License after Upgrade

After an upgrade, you must import license keys for each application you want to monitor.

To import and assign a license:

1 Login to **Policy Editor**.

2 Click **Module Manager**.

3 In **Licenses**, click the required application name.

4 Click **Import License Key**.

5 Browse and select the module license file.

6 Click **Import**.

Post Upgrade Configuration

Verify that the following settings are complete:

- "Updating the Keystore Password" on page 149
- "Setting the Polling Interval in Agent Manager" on page 150

Updating the Keystore Password

The `chg_keystore_pass.sh` script allows you to change the keystore passwords. As a security best practice, change the keystore passwords immediately after upgrading Change Guardian.

NOTE: Do not perform this procedure if Change Guardian server is in FIPS mode.

To change the keystore passwords:

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

2 Switch user to `novell`.

3 Go to the `/opt/novell/sentinel/bin` directory.

4 Run the `chg_keystore_pass.sh` script and follow the on-screen prompts to change the keystore passwords.

Setting the Polling Interval in Agent Manager

The heartbeat of Change Guardian Agent for Windows (displayed as Polling Interval) and Security Agent for UNIX (displayed as Heartbeat) determines the frequency at which Change Guardian server checks health of agents. It is the interval at which any policy changes on the server is synced to agents. If you have less than 500 agents and configured up to 15 policies per agent, consider setting **Polling Interval** to 15 minutes. If you have more than 500 agents or configured more than 15 policies per agent, consider setting the interval to 60 minutes. This ensures that there is no congestion of network traffic due to exchange of policy and agent health data at frequent intervals.

In Agent Manager, click **Manage Installation > Reconfigure**, and set the desired **Polling Interval**.

NOTE: This interval is referred to as Heartbeat in Policy Editor.

Verifying the Upgrade

To verify if the upgrade was successful, perform any of the following:

- Ensure that the server is running:

  ```
  netstat -an | grep LISTEN | grep 8443
  ```

- Verify that the latest packages are installed:

  ```
  rpm -qa | grep -i ncg
  ```

- Access the Change Guardian dashboard:

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

Troubleshooting

Deploying Alert Rules Fail

Issue: Deploying an alert rule fails when you create, modify, or delete an alert rule after an upgrade. Although Deployment Status shows Success, the Alert Rule Deployment Status window displays an error that deployment has failed.

Workaround:

To resolve the issue:

1. Comment the IP address 127.0.0.2 in the `/etc/hosts` file.
2. Restart the Change Guardian server:

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

Change Guardian Configuration Fails after Appliance Installation Completes

Issue: After appliance installation, configuration of Change Guardian might fail to complete with the following error message:

```
Change Guardian configuration has failed. Check /var/opt/novell/sentinel/
log/config_cg_onboot.log.
```

In such a case Agent Manager and `javos` services might fail to start.

Workaround: Reconfigure Change Guardian.

To reconfigure Change Guardian:

1. Verify if Change Guardian service (8443) is running using the command:

   ```
   netstat -an | grep "8443" | grep "LISTEN"
   ```

2. (Conditional) If Change Guardian service (8443) is not running, start Change Guardian service (8443):

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

3. Reconfigure Change Guardian:

   ```
   /opt/novell/sentinel/setup/configur.sh
   ```

Cleaning Up Data From PostgreSQL When Migration Fails

Issue: Database migration to PostgreSQL fails

Workaround: Delete the data that was partially moved to the PostgreSQL database.

To clear PostgreSQL:

1. Ensure that the PostgreSQL database is running.
2. Log in to the Change Guardian server as `root` and switch to `novell` user.
3. Go to the location where you have extracted the Change Guardian installer or the migration utility.
4. Delete the migrated data:

   ```
   ./db_migration_failure_cleanup.sh
   ```

5. (Conditional) If you are performing a traditional upgrading, upgrade Change Guardian.
6. (Conditional) If you are upgrading an appliance, run the appliance configuration utility.

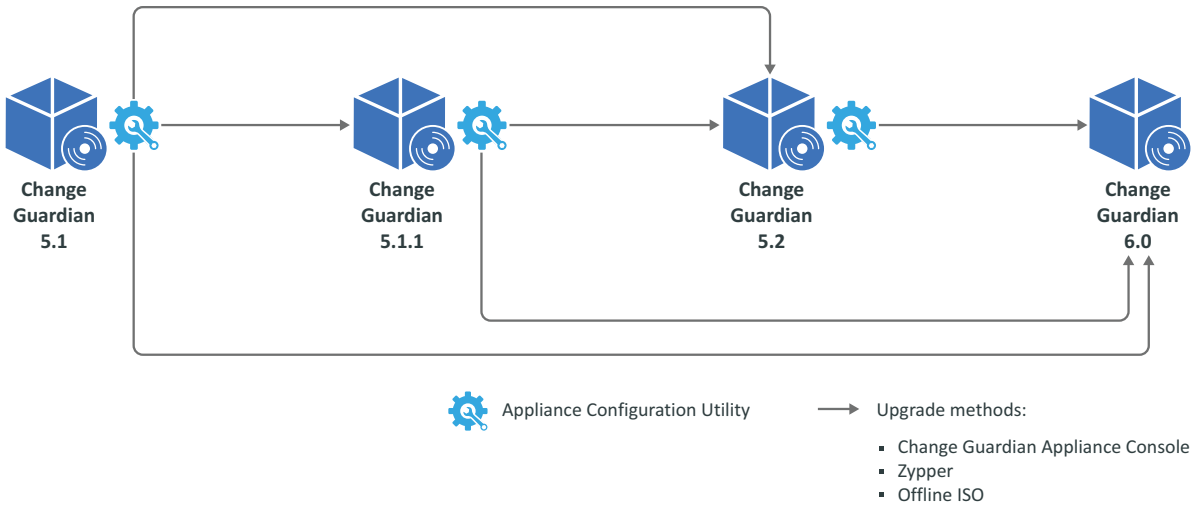
A Appendices

This chapter provides information about the following sections:

- "Appliance Upgrading Paths" on page 153
- "Uninstalling Change Guardian" on page 154
- "Configuring Auditing in UNIX or Linux" on page 157
- "Setting Up Assets for Monitoring" on page 161
- "Collecting Agent Logs Using Agent Manager" on page 168
- "Increasing Data Partition Size" on page 168
- "Migrating Agents to Agent Manager" on page 169
- "Services of the Security Agent for UNIX" on page 169
- "Troubleshooting" on page 170

Appliance Upgrading Paths

The following diagram illustrates the upgrade paths available for Change Guardian appliance, starting from version 5.1 to 6.0:



Review the following to understand the upgrade paths:

- Change Guardian 5.1 and Change Guardian 6.0 provides the base appliance image in ISO and OVF formats.

  You must have applied the channel updates to upgrade from Change Guardian 5.1 or later. The channel now lists the Change Guardian 6.0 updates.
- You can upgrade to a higher version using either of the following methods:
  - Change Guardian Appliance Console

- Zypper
- Offline ISO

Uninstalling Change Guardian

- "Uninstallation Checklist" on page 154
- "Uninstalling Change Guardian Event Collector Addon for Windows Agent" on page 154
- "Uninstalling Change Guardian Agent for Windows" on page 155
- "Uninstalling Security Agent for UNIX" on page 155
- "Uninstalling Policy Editor" on page 156
- "Uninstalling Change Guardian" on page 156
- "Post-Uninstallation Tasks" on page 156

Uninstallation Checklist

Use the following checklist to uninstall Change Guardian:

- Uninstall the following components before you uninstall Change Guardian:
  - Change Guardian Agent for Windows and Security Agent for UNIX using Agent Manager
  - Policy Editor
- Complete the post-uninstallation tasks to verify the Change Guardian uninstallation
- Uninstall assets before uninstalling Change Guardian and the components

Task	See
Uninstall the components	"Uninstalling Change Guardian Event Collector Addon for Windows Agent" on page 154
	"Uninstalling Change Guardian Agent for Windows" on page 155
	"Uninstalling Security Agent for UNIX" on page 155
	"Uninstalling Policy Editor" on page 156
Uninstall Change Guardian	"Uninstalling Change Guardian" on page 156
Perform the post-uninstallation steps	"Post-Uninstallation Tasks" on page 156

Uninstalling Change Guardian Event Collector Addon for Windows Agent

To uninstall, open the Change Guardian Event Collector Addon for Windows Agent application.

Uninstalling Change Guardian Agent for Windows

Ensure that you have removed assets using Agent Manager.

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

- “Uninstalling Remotely” on page 155
- “Uninstalling Manually” on page 155

Uninstalling Remotely

1. Log in as `administrator` to the Change Guardian server.
2. From the Administration Console, click **Integration > Agent Manager**.
3. Select the assets from which you want to uninstall the agent.
4. Select **Manage Installation > Uninstall Agents**.
5. Click **Start Uninstall**.

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 Security Agent for UNIX

Prerequisites:

- Reconfigure the agents using Agent Manger to disable the agent
- Remove assets from Agent Manager

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 the uninstallation is successful, 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 Uninstallation

Verify that the uninstallation is successful by performing the following:

- Check if all the components are uninstalled

  Run `vi` command on `/etc/vsaunix.cfg` configuration file to check if the agent for parameter 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

To uninstall:

1. Click **Asset Groups > *Agent_Name* > Remove**.
2. Go to **Control Panel > Programs and Features** and search for Change Guardian Policy Editor.
3. 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**.

Post-Uninstallation Tasks

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

Configuring Auditing in UNIX or Linux

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

- "Configuring a UNIX Auditing Subsystem" on page 157
- "Configuring a Linux Auditing Subsystem" on page 160

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

Configuring a UNIX Auditing Subsystem

This section provides information about configuring auditing on UNIX computers:

- "Configuring the AIX Audit Subsystem" on page 157
- "Configuring the HP-UX Audit Subsystem" on page 160
- "Configuring the Solaris Auditing Subsystem" on page 160

Configuring the AIX Audit Subsystem

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

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

To configure AIX audit subsystem:

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

```
bin:
     trail = /audit/trail
     bin1 = /audit/bin1
     bin2 = /audit/bin2
     binsize = 10240
  cmds = /etc/securitsy/audit/bincmds
stream:
  cmds = /etc/security/audit/streamcmds
classes:
     general =
USER_SU,PASSWORD_Change,FILE_Unlink,FILE_Link,FILE_Rename,FS_Chdir,FS_
Fchdir,FS_Chroot,PORT_Locked,PORT_Change,FS_Mkdir,FS_Rmdir,FILE_Symlin
k,USER_Exit,PROC_Create,PROC_Delete,FILE_Fchmod,FS_Rmdir,GROUP_User,GR
OUP_Adms,GROUP_Change,GROUP_Create,GROUP_Remove,USER_Remove,USER_Creat
e,USER_Chpass,USER_Change,FS_Mount,FS_Umount,FILE_Unlinkat,FILE_Symlin
kat
     Kernel =
PROC_Create,PROC_Delete,PROC_Execute,PROC_RealUID,PROC_AuditID,PROC_Re
alGID,PROC_Environ,PROC_SetSignal,PROC_Limits,PROC_SetPri,PROC_Setpri,
PROC_Privilege,PROC_Settimer,PROC_LPExecute,PROC_Adjtime,PROC_Kill
```

```
     files =
FILE_Open,FILE_Read,FILE_Write,FILE_Close,FILE_Link,FILE_Unlink,FILE_R
ename,FILE_Owner,FILE_Mode,FILE_Acl,FILE_Privilege,DEV_Create,FILE_Dup
fd,FILE_Chmod,FILE_Chown,FILE_Utimes,FILE_Truncate,FILE_Mknod,FILE_Sym
link,FILE_Unlinkat,FILE_Fchownat,FILE_Linkat,FILE_Fchown,FILE_Symlinka
t,FILE_Openxat,FILE_Mknodat,FILE_Renameat,FILE_Fchownat,FILE_Fchmod,FI
LE_Fchown,FILE_Fchmodat
     cron =
AT_JobAdd,AT_JobRemove,CRON_JobAdd,CRON_JobRemove,CRON_Start,CRON_Fini
sh
users:
     root = general,kernel,files,cron
     default = general,kernel,files,cron
role:
```

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

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

```
start

     binmode = off

     streammode = on
```

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

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

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

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

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

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

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

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

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

- FS_Mount
- FILE_Unlinkat
- CRON_Finish
- FILE_Linkat
- CRON_JobRemove
- PROC_Kill
- PROC_Execute
- FILE_Unlink
- FILE_Rename
- FILE_Fchown

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

5 Restart the audit subsystem.

6 Restart `detectd` service from the given location:

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

Configuring the HP-UX Audit Subsystem

The auditing subsystem on HP computers stores files in the `/etc/rc.config.d` directory. Ensure that the `/etc/rc.config.d/auditing` file includes the following lines:

```
AUDITING=1

PRI_AUDFILE=/.secure/etc/audfile1

PRI_SWITCH=1000

SEC_AUDFILE=/.secure/etc/audfile2

SEC_SWITCH=1000

AUDEVENT_ARGS1=" -P -F   -e admin -s exit -s kill -s vfsmount -s rename -s
unlink -s creat -s symlink -s fchown -s execv -s stime -s link -s
settimeofday -s mount -s clock_settime -s fchmod -s lchown -s umount2 -s
chmod -s execve -s chown -s open -s umount -s fork -s mknod -s vfork -s
chdir -s adjtime -s mkdir -s rmdir  "

AUDEVENT_ARGS2=" "
AUDEVENT_ARGS3=" "
AUDEVENT_ARGS4=" "
AUDOMON_ARGS=" -p 20 -t 1 -w 90"
```

Configuring the Solaris Auditing Subsystem

To configure on Solaris 10:

1. To ensure that the Basic Security Module restarts after reboot, run the following command from the `/etc/security` folder.

   ```
   ./bsmconv
   ```

2. Ensure that the `/etc/security/audit_control` file contains the following lines:

   ```
   flags: ua,fm,pc,fw,fr,ad,as,fc,ps,fd,nf
   naflags: fm,pc,fw,fr,as,ad,fc,ps,fd,nf
   minfree:20
   dir:/var/audit
   ```

To configure on Solaris 11:

1. Set the auditing flags as follows:

   ```
   auditconfig -setflags pm,ps,ua,as,fd,fc,fm,fw,fr
   auditconfig -setnaflags pm,ps,ua,as,fd,fc,fm,fw,fr
   ```

Configuring a Linux Auditing Subsystem

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

To configure:

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

```
chkconfig auditd on
```

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

2a Check if the audit process is running:

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

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

```
/sbin/auditd -s enable.
```

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

```
auditctl -e 1
```

NOTE: After you upgrade from Security Agent for UNIX 7.4 to 7.5, remove the system calls from the `/etc/audit/audit.rules` file that might have been added for Security Agent for UNIX 7.4.

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

Setting Up Assets for Monitoring

The following procedures are followed by the Micro Focus Quality Assurance team to setup the assets. Note the parameters to use later during the installation of Change Guardian Event Collector Addon for Windows.

- "Setting Up AWS" on page 161
- "Setting Up Office 365" on page 163
- "Setting Up Dell EMC" on page 164
- "Setting Up Exchange" on page 165

Setting Up AWS

This section provides the following information:

- "Setting the AWS Account" on page 161
- "Configuring CloudTrail" on page 162
- "Creating and Subscribing an Amazon Simple Queue Service (SQS)" on page 162
- "Important Parameters" on page 163

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

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

Setting the AWS Account

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

To setup:

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

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

   NOTE: The file contains the **Access Key ID** and **Secret Access Key** that you have to use when installing the connector.

   ---
8. Click **Groups > *group_name* > Group Action > Add Users to Group**.
9. Select the users to add to the group and click **Add Users**.
10. To view or create an Access key ID, open user summary and click **Security Credentials > Create Access key**.

Configuring CloudTrail

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

To configure CloudTrail:

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

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

Creating and Subscribing an Amazon Simple Queue Service (SQS)

To create an SQS:

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

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

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

Important Parameters

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

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

Setting Up Office 365

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

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

Registering the Application in Azure AD

To register:

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

2 Click **Azure Active Directory**.

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

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

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

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

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

6 Click **API permissions > Add a permission > Office 365 Management APIs > Delegated permissions and Application Permissions**.

7 Select **ActivityFeed.Read**, **ActivityFeed.ReadDlp** and **ServiceHealth.Read** and click **Add permissions**.

8 On the API permissions page, click **Grant admin consent for <*organization name*>**.

Important Parameters

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

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

Setting Up Dell EMC

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

Installing Common Event Enabler

To install Common Event Enabler (CEE):

1 Log into the machine with the account that has administrator privilege.

2 Ensure that .NET Framework 3 is enabled.

3 Run the file `EMC_CEE_Pack` for either the 32-bit (WIN32) or the 64-bit (X64) version of the software.

4 Follow the prompts and complete the installation.

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

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

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

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

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

9 Restart the machine.

10 Access the CEPA server from a browser.

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

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

To set up application access:

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

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

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

Important Parameters

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

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

Setting Up Exchange

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

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

This section provides the following information:

- "Enabling Mailbox Audit Logging" on page 166
- "Enabling Administrator Audit Logging" on page 166
- "Enabling Execution of Microsoft Exchange PowerShell Scripts" on page 167
- "Configuring Microsoft Exchange PowerShell" on page 167
- "Locating the Fully Qualified Domain Name" on page 167
- "Important Parameters" on page 167

Enabling Mailbox Audit Logging

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

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

- Enable mailbox audit logging for Ben Smith's mailbox:

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

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

  ```
  Set-Mailbox -Identity "Ben Smith" -AuditDelegate SendAs,SendOnBehalf -AuditEnabled $true
  ```
- Specify that the MessageBind and FolderBind actions performed by administrators are logged for Ben Smith's mailbox:

  ```
  Set-Mailbox -Identity "Ben Smith" -AuditAdmin MessageBind,FolderBind -AuditEnabled $true
  ```
- Specify that the HardDelete action performed by the mailbox owner will be logged for Ben Smith's mailbox.

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

Enabling Administrator Audit Logging

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

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

- Enable administrator audit logging:

  ```
  Set-AdminAuditLogConfig -AdminAuditLogEnabled $True
  ```
- Enable administrator audit logging for every cmdlet and every parameter in the organization, with the exception of Get Cmdlets:

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

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

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

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

Enabling Execution of Microsoft Exchange PowerShell Scripts

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

To enable:

1. Open **Local Group Policy Editor.**
2. Go to **Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components > Windows PowerShell**.
3. Set **Turn on Script Execution** to Enabled.
4. Set **Execution Policy** to **Allow local scripts and remote signed scripts**.

Configuring Microsoft Exchange PowerShell

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

To allow the services to run as a domain administrator:

1. Open Windows services, and select **ArcSight Microsoft Exchange PowerShell**.
2. Open **Properties**, click **Log On**.
3. Click **This Account > Browse > Locations**, and select the domain name.
4. Specify the domain administrator credentials.

Locating the Fully Qualified Domain Name

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

Important Parameters

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

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

Collecting Agent Logs Using Agent Manager

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

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

To collect agent logs:

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

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

Increasing Data Partition Size

You can increase the data partition to suit the sizing need of Change Guardian server:

To increase the partition size:

1. Add a hard disk to the virtual machine.
2. Stop the Change Guardian services by running the following command: `rcsentinel stop`
3. Run the following command to list the partition that was added: `fdisk -l`
4. Format the new disk to ext3 file system by running the following command: `mkfs.ext3 /dev/<partition1>`
5. Create a temporary directory `/tmp/new` to copy files from `/var` or `/opt`.
6. Mount new partition to the temporary directory by running the following command: `mount /dev/<partition1> /tmp/new`
7. Move the data directory to the newly created directory. For example: `mv /var/opt/* /tmp/new`
8. Unmount the temporary directory by running the command: `umount /tmp/new/`

9 Mount the new partition to /var/opt/ by running the command: `mount /dev/partition1 /var/opt/`

10 Confirm that the data partition `/var/opt` is mounted by running the command: `mount`

11 Verify that the data partition `/var/opt` has moved to the new partition by running the command: `df -h`

Migrating Agents to Agent Manager

If you plan to use Agent Manager to manage all agent deployments, migrate the agents from UNIX Agent Manager to Change Guardian Agent Manager. Ensure that you have UNIX Agent Manager to 7.5 or later.

To migrate the agents to Agent Manager:

1 In UNIX Agent Manager, navigate to **All Hosts** window and select the agent that you want to export.

2 Navigate to **Manage Hosts > Import/Export Host Lists**.

3 From the Export area select one of the following:

- Selected Hosts
- All Hosts

4 Click **Save**.

5 Log in to the Change Guardian server as an `administrator`.

6 From the User defined groups, click **Add Assets**.

Or

Select **All Assets > Manage Assets > Add > Host List**.

7 Browse to the location where you have saved the exported agent list.

8 Select the `<Host_list>.hosts` file to import the agent to Agent Manager.

Services of the Security Agent for UNIX

The following are key processes that are used to validate the agent services installation and methods used for start and stop the agent services:

- `detectd`: Performs monitoring tasks and data retrieval. The behavior of this process is directed by the content of the `detect.xml` file.
- `Nqmagt`: Monitors the status of the other Agent processes and restarts them if necessary. This process should run continuously after the Agent is installed.
- `rclink`: Starts the Agent processes immediately after the deployment process and adds a startup script to the `/etc/rc.d` directory. This startup script starts the Agent processes after each reboot when the master `rc` script runs. This is the default method, and should be used in nearly all environments.
- `inetd`: Starts the Agent processes immediately after the deployment process and adds an entry to the `/etc/inittab` file. This `inittab` file entry starts the Agent processes at the default run level after each reboot.

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.

- "Configuring Change Guardian Appliance to Boot Normally" on page 170
- "Administration Console is Blank on Internet Explorer After Logging in" on page 171
- "Change Guardian Agent for Windows Installation Using Agent Manager Fails" on page 171
- "Asset Monitoring Failure Reports are not Captured for All Event Types" on page 172
- "Azure AD Monitoring Events are not Captured for All Event and Attribute Types" on page 172
- "Manual Configuration Required to use Registry Browser" on page 172
- "Restarting the Change Guarding server with FIPS Mode Enabled Logs an Exception" on page 173
- "Change the Agent Package Version" on page 173
- "Installing Change Guardian Agent for Windows Fails with SMB Protocol Mismatch" on page 173
- "Change Guardian Web Console is Blank if the License Has Expired" on page 173
- "Change Guardian is not Receiving Events from Dell EMC" on page 174
- "Unable to Browse File Locations and AD Using Policy Editor File Browser" on page 174
- "Troubleshooting Agents in Warning State" on page 174
- "AD Certificate is not Signed by a Well Known CA" on page 176
- "Cannot Connect to AD Hostname, Domain, or IP Address" on page 177
- "Security Agent for UNIX" on page 177

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 A-1 *Modifying Disk UUIDs*

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

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

- **/etc/fstab**

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

- **/etc/default/grub**

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

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

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

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

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

Administration Console is Blank on Internet Explorer After Logging in

Issue: If the Internet Security Level is set to High, a blank page appears after logging in to Sentinel and the file download pop-up might be blocked by the browser.

Workaround: Set the security level to Medium-high and then change to Custom level as follows:

To change the settings:

1 Navigate to **Tools** > **Internet Options** > **Security** and set the security level to **Medium-high**.

2 Make sure that the **Tools** > **Compatibility View** option is not selected.

3 Navigate to **Tools** > **Internet Options** > **Security tab** > **Custom Level**, then scroll down to the **Downloads** section and select **Enable** under the **Automatic prompting for file downloads** option.

Change Guardian Agent for Windows Installation Using Agent Manager Fails

Issue: Change Guardian Agent for Windows installation using Agent Manager fails and displays the following error in the failed task logs:

```
protocol negotiation failed...
```

This error might occur due to following reasons:

- SMB1 protocol is disabled on Change Guardian Agent for Windows.
- Change Guardian server is installed on SLES 11 SP4 or RHEL 6.7 platforms which supports SMBv1 only.

Workaround: Install Change Guardian Agent for Windows manually. For more information see "Manual Installation" on page 33.

Asset Monitoring Failure Reports are not Captured for All Event Types

Issue: The Asset monitoring failure reports are not captured for all event types, such as audit failures, registry failures or system failures.

Workaround: To view the failure reports you must apply the policy where auditing mechanism of the specific event mentioned in the policy has failed.

Azure AD Monitoring Events are not Captured for All Event and Attribute Types

Issue: When you upgrade Change Guardian 5.0 to Change Guardian 5.1 or later, Change Guardian server is unable to fetch events for the newly added events and attributes. The events are not captured if you have selected "All Events" or "All Attributes" when you created the policy using Change Guardian 5.0.

Workaround: Perform the following procedure to overcome this issue:

1. . In the left pane of the Policy Editor window, select Azure Active Directory > Azure Active directory Policies.
2. Expand the Azure Active directory Policies and select the policy where you are monitoring "All Events" or "All Attributes".
3. Click Edit and modify the description.
4. Click Submit.
5. Enable the policy revision.

Manual Configuration Required to use Registry Browser

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

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

Restarting the Change Guarding server with FIPS Mode Enabled Logs an Exception

Issue: If the Change Guardian server is FIPS-mode enabled and the server is restarted, the server logs an error message:

```
"An unexpected exception occurred while decrypting data failed. Root cause:
CKR_ENCRYPTED_DATA_INVALID (sun.security.pkcs11.wrapper.PKCS11Exception)
java.security.ProviderException: doFinal() failed"
```

(Bug 1129167)

Workaround: You can ignore the exception.

Change the Agent Package Version

Issue: You 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`.

Installing Change Guardian Agent for Windows Fails with SMB Protocol Mismatch

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

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

The error might occur due to the following reasons:

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

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

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

Change Guardian Web Console is Blank if the License Has Expired

Issue: If your Change Guardian license expires, the web console displays a blank page. (Bug 949208)

Workaround: Add the license through the command line by using the `softwarekey.sh` script. For more information, see *Adding a License Key* in the *Change Guardian User Guide*.

Change Guardian is not Receiving Events from Dell EMC

Issue: Change Guardian does not receive Dell EMC events if the CEPA server is not running. Accessing the CEPA from a browser shows that the site cannot be reached.

Workaround:

Start the CEPA server:

1. Open `services.mcs` and run the EMC CAVA service.
2. In the Dell EMC web-console, check if the CEPA IP is provided in the following format: `http://1.1.1.1:12228/cee`

Unable to Browse File Locations and AD Using Policy Editor File Browser

Issue: Following are the conditions:

- Unable to browse to file locations within a policy.
- Unable browse active directory from within a policy. (Bug 995355)

Workaround: To enable LDAP browsing in policy editor, perform the steps mentioned in NetIQ Knowledgebase Article 7017291.

Troubleshooting Agents in Warning State

The following table gives you information about how to resolve the agent issues reported in the agent health dashboard:

Issue as shown the Dashboard	Error Code	Workaround
Driver initialization failure	Change Guardian Agent for Windows: 00002053 Group Policy: 00001546 AD: 00000778	Check if the driver is loaded in the registry
Driver Configuration failure	Change Guardian Agent for Windows: 00002052 Group Policy: 00001546 AD: 00000778	Check if the driver registry key is set for the specific policy
General Error setting up monitoring policy	Change Guardian Agent for Windows: 00002053	Check if the policy is loaded in the registry

Issue as shown the Dashboard	Error Code	Workaround
Unable to write to baseline	Change Guardian Agent for Windows: 00002053	Check if the system has read and write permissions in the following folder: `C:\Program Files (x86)\NetIQ\ChangeGuardianAgent\data\CGW_Repository`
Missing auditing for 'User Account Management', unable to monitor policy	AD: 00000774	Check if AD auditing is configured
Missing auditing for 'Computer Account Management', unable to monitor policy	AD: 00000774	Check if AD auditing is configured
Missing auditing for 'Distribution Group Management', unable to monitor policy	AD: 00000774	Check if AD auditing is configured
Missing auditing for 'Security Group Management', unable to monitor policy	AD: 00000774	Check if AD auditing is configured
Missing auditing for 'Authorization Policy Change', unable to monitor policy	AD: 00000774	Check if AD auditing is configured
Missing auditing for 'Authentication Policy Change', unable to monitor policy	AD: 00000774	Check if AD auditing is configured
Missing auditing for 'Directory Service Changes', unable to monitor policy	AD: 00000774 Group Policy: 00001542	Check if AD auditing is configured
Missing auditing for 'Directory Service Access', unable to monitor policy	AD: 00000774 Group Policy: 00001542	Check if AD auditing is configured for both AD and Group Policy
Missing failure auditing for 'User Login Monitoring', unable to monitor logon failure policy	AD: 00000774	Check if AD auditing is configured
Missing success auditing for 'User Login Monitoring', unable to monitor logon success policy	AD: 00000774	Check if AD auditing is configured
Missing failure auditing for 'User Logoff Monitoring', unable to monitor logoff failure policy	AD: 00000774	Check if AD auditing is configured
Missing success auditing for 'User Logoff Monitoring', unable to monitor logoff success policy	AD: 00000774	Check if AD auditing is configured

Issue as shown the Dashboard	Error Code	Workaround
Failed to read Active Directory object <directory_path>, unable to monitor policy	AD: 00000779 Group Policy: 00001547	Check if AD auditing is configured
Missing auditing flags <\flag_value> in ACE SACL for <directory_path>, unable to monitor policy	AD: 00000776 Group Policy:00001544	Check if AD auditing is configured
Required provider IQCGW missing	Change Guardian Agent for Windows: ELQ0006	Check if the registry key of the provider includes the value `IQCGW`
Required provider IQCG missing	Change Guardian Agent for Windows: ELQ0006	Check if the system is a domain controller and check if the registry key of the provider includes the value `IQCG`
Required provider CGADProvider is missing	AD: ELQ0006	Check if the system is a domain controller and check if the registry key of the provider includes the value `CGADProvider`
Required provider CGSmartProvider is missing	Change Guardian Event Collector Addon for Windows: ELQ0006	Check if Change Guardian Event Collector Addon for Windows Agent is enabled in Agent Manager before installing Change Guardian Agent for Windows
Required provider CGAzureADProvider is missing	Azure AD: ELQ0006	Check if Azure AD monitoring is enabled in Agent Manager before installing Change Guardian Agent for Windows

AD Certificate is not Signed by a Well Known CA

Workaround: Use a certificate signed by a well known CA.

If you used a certificate that was not signed by a well known CA, then import the certificate to a Java keystore.

To import the certificate:

1. Go to `/opt/novell/sentinel/jdk/jre/lib/security`.
2. Download and copy the AD certificate to the Change Guardian server.
3. Import the certificate:

   ```
   /opt/novell/sentinel/jdk/jre/bin/keytool -import -alias <alias_name> -file <AD_certificate_path> -keystore /opt/novell/sentinel/jdk/jre/lib/security/cacerts -storepass changeit
   ```

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 the `server.conf` file:

1. Open the file `/etc/opt/novell/sentinel/config/server.conf`.
2. Add the following text next to `wrapper.java.additional.74=`

   `-Dcom.sun.jndi.ldap.object.disableEndpointIdentification=true`
3. Go to `/opt/netiq/cg/scripts`.
4. Restart the services:

   `./cg_services.sh restart`

Security Agent for UNIX

This section provides information about the following issues:

- "Unable to Connect to Port" on page 177
- "Unable to Run the Services" on page 177
- "Policies Are Not Applied to the Agent" on page 178
- "Events are not Displayed in the Events Dashboard" on page 178
- "Events Not Generated When Write Permissions Are Modified" on page 178
- "Events are not Generated After Configuring Security Agent for UNIX" on page 178
- "Cannot Browse User While Creating Policies" on page 179
- "Events are not Generated After Password Change" on page 179

Unable to Connect to Port

Issue: Security 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: Agent services are not running.

Workaround:

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

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

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

2a Restart `vigilentagent` service:

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

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

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

2c Restart `auditd` service:

```
service auditd restart
```

Policies Are Not Applied to the Agent

Issue: The policies are not applied to the agent 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 Displayed in the Events Dashboard

Issue: Events are not generated even though all the configuration settings are successful.

Workaround: Verify if the spool file entry is frequently updated when events are not generated even though all the configuration settings are successful in the following directory:

```
/usr/netiq/vsau/local/spool/LinuxAuditObject__singleton/*.udetect_events
```

Events Not Generated When Write Permissions Are Modified

Issue: When you modify the write permission corresponding to rule group of a file, Change Guardian fails to generate events for file monitoring.

Workaround: It is recommended that you do not modify file permissions.

Events are not Generated After Configuring Security Agent for UNIX

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

Workaround: Ensure that the following is set:

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

Cannot Browse User While Creating Policies

Issue: User Browse option does not work while creating policies using Policy Editor.

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

To enter the data source paths:

1. (Conditional) If your operating system is 32-bit, in the registry `\HKLM\Software\NetIQ\ChangeGuardianAgent\repositoryEnabled` set the `repositoryEnabled` flag to 1.
2. (Conditional) If your operating system is 64-bit, in the registry `\HKLM\SOFTWARE\Wow6432Node\NetIQ\ChangeGuardianAgent\repositoryEnabled` set the `repositoryEnabled` flag to 1.
3. Restart the Change Guardian Agent for Windows.

Events are not Generated After Password Change

Issue: After you change the Change Guardian password, events are not generated because the REST dispatcher password is not updated in Policy Editor. (`Bug 1121890`)

Workaround: Enter the new password for the REST dispatcher by using Policy Editor, then reconfigure the Change Guardian server.