User Guide

Change Guardian™ 6.0

July 2020

NetIQ

Legal Notice

© Copyright 2019 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 5

1 Introduction 7

Dashboards . . . 7
- Change Guardian Dashboard . . . 7
- Threat Response Dashboard . . . 7

Administration Console . . . 8

2 Analyzing Change Events 9

Overview . . . 9
Examples of Using the Change Guardian Dashboard . . . 9
- Example- Analyzing the Data in the Chart View . . . 10
- Example- Analyzing the Data in the Grid View . . . 10

Managing Data in the Change Guardian Dashboard . . . 10
- Filtering and Grouping Event Data . . . 10
- Viewing Event Details . . . 11

Customizing the Change Guardian Dashboard . . . 11

3 Viewing All Events 13

Searching Events . . . 13
- Performing a Search . . . 14
- Viewing Search Results . . . 15
- Refining Search Results . . . 17
- Saving a Search Query . . . 19
- Exporting the Search Results to a File . . . 23

Filtering Events . . . 23
- Creating Filters . . . 24
- Sample Filters . . . 27
- Viewing Events by Using Filters . . . 29
- Managing Filters . . . 29

Tagging Events . . . 29
- Creating a Tag . . . 30
- Viewing Tagged Events . . . 30
- Managing Tags . . . 31
- Performing Text Searches for Tags . . . 32
- Deleting Tags . . . 32
- Associating Tags with Objects . . . 32

Executing Actions . . . 33
Viewing Vulnerabilities . . . 33

4 Viewing Identity Data 35

Performing a Search . . . 35
- Using the Search Box . . . 35
- Using the Search Fields . . . 35

Viewing Profile Details . . . 36
Viewing Activities . . . 37
Searching and Viewing User Identities . . . 37

5 Analyzing Alerts **39**

Analyzing Alerts in the Threat Response Dashboard and Alerts View 39
Viewing Alerts in the Alert Dashboard 41
Viewing Alerts 42
Troubleshooting 43
Unable to View Alerts in the Dashboard and Alert Views 43

6 Managing Reports **45**

Creating Reports 46
Scheduling Reports 46
Scheduling Reports Across Change Guardian Servers 46
Saving Reports in the CSV Format 47
Working with Reports 47
Rebranding Reports 48

About this Book and the Library

The *User Guide* provides information about the tasks that can be performed by a Change Guardian user who analyzes the change events.

Intended Audience

This book is intended for Change Guardian users such as analysts, operators, and other users.

Additional Documentation

The Change Guardian documentation library includes the following resources:

Installation and Administration Guide

Provides information for Change Guardian administrators who are responsible for understanding Change Guardian product concepts, and installing and using this operational change auditing solution for their enterprise network.

Release Notes

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

1 Introduction

Change Guardian provides multiple web-based user interfaces to allow you to access data. Change Guardian captures the change events that occurred in the systems it is monitoring through policies.

Change Guardian provides the following user interfaces through which you can view the event details, search events, view alerts, manage dashboard, and many more.

- "Dashboards" on page 7
- "Administration Console" on page 8

Dashboards

Change Guardian provides the following dashboards:

- "Change Guardian Dashboard" on page 7
- "Threat Response Dashboard" on page 7

Change Guardian Dashboard

This dashboard provides the following information:

Dashboard: Change events and event details

Policy: Reports about policies and policy sets that are associated with agents and agent groups

Agents: Health status of agents and access to Agent Manager

You can navigate to the other user interfaces from Change Guardian dashboard.

To access the Change Guardian dashboard:

1. Open the following URL in a web browser: `https://<IP_Address_Change_Guardian_server:8443>`

For more information, see Chapter 2, "Analyzing Change Events," on page 9

Threat Response Dashboard

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

You can use this dashboard to view and triage all events. Any user with permission to manage alerts can use the dashboard.

To open the Threat Response Dashboard, click **Manage Alerts** in the Change Guardian dashboard. For more information, see Chapter 5, "Analyzing Alerts," on page 39.

Administration Console

You can use this interface to view and interact with Change Guardian data. You can perform tasks such as the following:

- Search events and save search results.
- Export event details to a file.
- View alerts.

To access Administration Console, click **Administration** in the Change Guardian dashboard.

2 Analyzing Change Events

This chapter provides information about how to analyze the change events.

- "Overview" on page 9
- "Examples of Using the Change Guardian Dashboard" on page 9
- "Managing Data in the Change Guardian Dashboard" on page 10
- "Customizing the Change Guardian Dashboard" on page 11

Overview

The Change Guardian dashboard provides information about change events in a chart view and a grid view.

Chart View In the chart view you can get the following information:

- Events generated for each application
- Events based on severity
- The users and assets that generated the most events
- The most common events, and the most common policy violation that resulted in events
- Filtered view of the above based on the number of days

Grid View In the grid view, you can find the event details that includes who initiated the change, what is the change, and where the change occurred.

NOTE: The GenerationTime column provides the timestamp at which an action was performed on the asset, while EventTime provides the timestamp at which Change Gaurdian collected the corresponding event. To view the time stamp for UNIX events add EventTime column.

In the grid view, you can filter events by grouping events by their severity, name, time stamp, and so on. You can add or removed columns and group the events by any column name and export it to a XLS file.

Examples of Using the Change Guardian Dashboard

This section gives examples of using the Chart View and the Grid View.

- "Example- Analyzing the Data in the Chart View" on page 10
- "Example- Analyzing the Data in the Grid View" on page 10

Example- Analyzing the Data in the Chart View

Arvanti is responsible for the organization's Active Directory server. She uses Change Guardian to monitor changes happening on the Active Directory deployment by using the Change Guardian dashboard. She uses the default filter to view all the unmanaged or unauthorized events of the previous day.

One morning, Arvanti finds that the chart view displays an increase in the average number of change events in the past one day. She reviews events dashboard specific to the Active Directory, and observes that these set of change events are initiated by three users. She reviews the Top Users list and the Top Events, and finds that there are higher than usual “User account was created” event. She selects the “User account was created” event to analyze the event details and investigate all “User account created” events in the last one day.

Example- Analyzing the Data in the Grid View

Mandy routinely analyzes change events and prefers to directly work with event data. One day she gets an input from her peer that there had been some unusual activities on the Microsoft Exchange server over the weekend, mostly on Sunday.

Mandy opens the Change Guardian dashboard and modifies the filter to view all change events from Sunday 6:00 a.m. to 6:00 p.m. She selects the Microsoft Exchange events and switches to Grid View.

In the Grid View, Mandy first groups events by Event Name. She observes that there are unusually higher number of “Mailbox Create and Mailbox Delete” events. To get into further details, Mandy expands the list of “Mailbox Create” events and starts reviewing the details of each event such as, who created the mailbox, what mailbox was created, from where the user logged in, and what time this event occurred. Mandy identifies one suspicious user who made multiple changes and she modifies the filter back to past one week to view the events made by the suspicious user. She reviews all the activities performed by the user to analyze for any security breach.

Managing Data in the Change Guardian Dashboard

The dashboard allows you to filter, group, and sort events and displays event details.

- “Filtering and Grouping Event Data” on page 10
- “Viewing Event Details” on page 11

Filtering and Grouping Event Data

The chart displays the total number of users that contributed to event with a severity, the number of assets on which the event was triggered, the kind of change that triggered the event, and the policies that the events violated.

You can narrow your search by filtering the events by application type, severity, time, and so on. Similarly you can group the event by users, change category, or by the event attribute presented as column names in the grid view.

Viewing Event Details

You can view who triggered an event, where the event was generated from, what are the changes made. Besides these details you can view the severity, the policy that was violated, the domain in which the change occurred. To view every details of an event, on the grid view click on a event row. This opens the Event Details page.

NOTE: For AWS Identity and Access Management (IAM), the target host displays the AWS region name, which is the domain name for AWS IAM.

You can manipulate the Grid View by adding or removing columns to the view. You can export the view to a spreadsheet (`.xls` format). Similarly, you can set a new time range to filter events by.

Customizing the Change Guardian Dashboard

You can use the Settings options to customize the dashboard to suit your requirements. For example, you can customize the dashboard to view only the licensed applications.

3 Viewing All Events

Use the Administration Console to search and view events, configure filters and tags on events, export search results to files, refine event search by users, and view the vulnerability data about the events.

By default, the Administration Console displays events with all severity levels, allowing you to view the following information for each event:

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

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

This chapter provides the following information:

- "Searching Events" on page 13
- "Filtering Events" on page 23
- "Tagging Events" on page 29
- "Executing Actions" on page 33
- "Viewing Vulnerabilities" on page 33

Searching Events

Change Guardian provides an option to perform a search on events. With the necessary configuration, you can also search system events generated by Change Guardian and view the raw data for each event. By default, events are returned in a reverse chronological order.

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

You can run a search to view events indexed in traditional storage. You can also search for events in other Change Guardian servers that are distributed across different geographic locations.

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

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

- `pn:NMAS AND sev:5`

  This searches for events with the product name NMAS and severity five.
- `sip:10.0.0.01 AND evt:"Set Password"`

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

Multiple advanced search criteria can be combined by using various operators. The advanced search criteria syntax is modeled on the search criteria for the Apache Lucene open source package.

NOTE: If time is not synchronized across your server, client, and event sources, you might get unexpected results from your search. This is especially a problem if searches are performed on time durations such as **Custom**, **Last 1 hour**, and **Last 24 hours** where display results are based on the time zone of the machine on which the search is performed.

Following sections provide information about the following:

- “Performing a Search” on page 14
- “Viewing Search Results” on page 15
- “Refining Search Results” on page 17
- “Saving a Search Query” on page 19
- “Exporting the Search Results to a File” on page 23

Performing a Search

To search events, perform the following steps.

To perform a search:

1. Log in to the Administration Console:

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

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

- **Select and Append criteria:** Click **Select and Append criteria** and select from the criteria listed, click **Add**, and then click **Search**. You can select criteria from the list of criteria or filter the criteria based on recent criteria, tags, or filters.
  - **Show only recent criteria:** Select a search criterion from the recent search history. The search history displays a maximum of 15 search expressions. Select the criteria, click **Show recent criteria**, and then click **Add**.
  - **Show only Filters:** You can reuse existing filters to perform a new search. Click **Show Filters** that lists the existing filters. Select the filter on which you want to perform the search, and then click **Add**.
  - **Show only Tags:** You can search events that have a particular tag. Click **Show Tags**, that lists the tags in the system. Select the tags, and then click **Add**.

  You can combine multiple criteria, tags, or filters by using the **And** or **Or** condition.

4. (Optional) Select a time period for the search.
   - The default is **Last 1 hour**.
   - **Custom** allows you to select a start date and time and an end date and time for the query. The start date should be earlier than the end date, and the time is based on the machine's local time.
   - **Whenever** searches all available data, without any time constraints.
5. (Optional) If you have administrator privileges, you can select other Change Guardian servers for the search.

   If you have data federation configured, you can perform a search on other Change Guardian servers. For more information, see Configuring Data Federation in the "*Change Guardian Installation and Administration Guide*".
6. Click **Search**.

   The search results are displayed. For information on the search results, see "Viewing Search Results" on page 15.
7. (Optional) Modify the search criteria by clicking **Edit Criteria**.
8. (Optional) Modify the search results by selecting the desired event fields in the search results

   To add an AND or Or condition to the existing criteria, left-click the event field, select the required fields, and then specify the desired condition.
9. Click **Search**.
10. (Conditional) To save the search query, see "Saving a Search Query" on page 19.

Viewing Search Results

Searches return a set of events. When results are sorted by relevance, only the top 50,000 events can be viewed. When results are sorted by time, all the events in the system are displayed.

Occasionally, the search engine might index events faster than they are inserted into the data directory. If you run a search that returns events that were not added in the data directory, you get a message indicating that some events match the search query, but they are not found in the `data` directory. If you run the search again later, the events are added to the `data` directory and the search is shown as successful.

To see detailed event information, click the shield icon.

The information in each event is grouped into the following categories:

Category	Icon	Description
General	No icon	Generic information about the event, such as severity, date, time, product name, and taxonomy.
Initiator		The source that caused the event to occur. The source can be a device, network port, etc.
Target		The object that is affected by the event. The object can be a file, database table, directory object, etc.
Observer		The service that observed the event activity.
Reporter		The service that reported the event activity.
Tags	No icon	Tags that the events are being tagged with.
Customer value	No icon	Fields set by the customer.
Retention period	No icon	Retention period of the event.

The initiator, target, and observer can be hosts, services, and accounts. In some cases, the initiator, target, and observer can be all the same, such as a user modifying this or her own account. In other cases, the initiator, target, and observer can be different, such as an intrusion detection system detecting a network attack. If an event field has no data, it is not displayed in the results.

Event fields are grouped according to the following categories:

Group	Icon	Description
Host		The initiator or target host information. For example, initiator host IP, target hostname, or target host ID.
User		The initiator or target user information. For example, the initiator username, initiator user department, target user ID, or target username.
Service		The initiator or target service information. For example, the target service name, target service component, or initiator service name.
Domain		Domain information of both the host and user. For example, the target host domain and initiator username.
IPCountry		The country information of the initiator and target trust. For example, the target host country.
Target trust		The target trust and target domain information of the event that was affected. The name can be a group, role, profile, etc.
Target data		The target data name and data container information. The data name is the name of the data object, such as a database table, directory object, or file that was affected by the event. The data container is the full path for data object.
Tenant name		The name of the tenant that owns the event data, applied to all the events in the inbound stream from a given Collector. The tenant name can be the name of the customer, division, department, etc.
Vulnerability		A flag that indicates whether Exploit Detection has matched this attack against known vulnerabilities in the target.

Each event type is represented by a specific icon. The following table lists the icons that represent the various types of events:

You can view the search results in the summary view and in the detailed view. When you mouse over an event field, the information about the field is displayed.

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

Summary View

The Summary view of the search results displays the basic information about the event. The basic information includes severity, date, time, product name, taxonomy, and observer category for the event.

Detailed View

1. To view the report details, click the **More** link at the top right corner of the search results.

   This displays details such as host/user domain information, IPCountry information, extended target fields like TargetTrust and TargetData, Observer and Reporter fields, customer set variables, default data retention duration information for any individual event, and the tags set for the event.
2. To view all the details of an event, click the **All** link.
3. To view details about all events, click the **Show more details** link at the top of the search results page.

   You can expand or collapse the details for all events on a page by using the **Show more details** or **Show less details** link.

Refining Search Results

The search refinement panel can be used to narrow the search results by selecting one or more values for an event field. You can refine the results for one or more event fields.

The set of event fields that is displayed in the search refinement panel is configurable on a per-user basis.

For performance considerations, the maximum sample size used to calculate the event field value statistics is 50,000 events. The actual sample size is displayed in the field count label as `Field counts based on the first <sample-size> events` where `<sample-size>` is replaced by the actual sampling size.

To refine search results:

1. Log in to the Administration Console:

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

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

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

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

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

5 To refine the search, select the event fields from the available fields, then click **Save**.

The selected event fields are displayed in the **REFINE** panel.

A count at the right side of each event field displays the number of unique values that exist for that event field in the data directory. The calculation is based on the first 50,000 events found.

The event field selection is on a per-user basis. Each user can have a different set of selected event fields.

6 Click each event field to view the unique values for that event field.

For example, if the search results contain events that had severities 1, 2, 5, and 4, the event field is displayed as **Severity (4)**.

The top 10 unique values are initially displayed in the order of most frequent to least frequent.

The value next to the check box represents the unique value for that event field and the value at the far right represents the number of times the value appears in the search result.

If there are multiple unique values occurring the same number of times in a search, the values are sorted by the most recent occurrence of the value.

For example, if events of severity 1 and 4 occurred 34 times in the search results, and an event of severity 4 was logged most recently, the unique value 4 appears at the top of the list.

To display the unique values in the order of least frequent to most frequent, click **reverse.**

When there are more than 10 unique values, you can view and filter either the top 10 or the bottom 10 unique values. You cannot refine your search on both the conditions at the same time.

In the following scenarios, the number of events returned from a refined search is greater than the number of values listed for an event field:

- If the refinement performs a new search with additional terms intersected with the initial search string, such as by using an AND operator, the new search is run against all events in the system, including the result set from the initial search. If new events that came into the system match the refined search, they are shown in the resulting set and the event count is greater than the field value count.
- If there are more than 50,000 events, the event field statistics are calculated only on the first 50,000 events.

  There could be an event field value that occurs 50 times in the first 50,000 events, but it could occur 1,000 times in all other stored events. In this scenario, the displayed value count is 50, but when the search is refined with this value it returns 1,000 events.

7 Click **OK**.

Selected event field values are listed under the event field in the **REFINE** panel.

The right panel displays the refined search results, which contain only the selected values.

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

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

10 (Optional) Click **add to search** to add the refined search values to the current search tab and to recalculate the search statistics.

If you have already added the event field value to the current search tab, clicking **clear** does not return to the previous search results.

Saving a Search Query

You can save a search query, then repeat it as desired. To save a search query, you must first perform a search. When you are satisfied with the search results, you save the search query.

NOTE: You must have the necessary permission to access the specific options. For example, only users in the Report Administrator role can save the search query as a report template.

- "Saving a Search Query as a Search Template" on page 19
- "Saving a Search Query as a Filter" on page 19
- "Saving a Search Query as a Report Template" on page 20
- "Saving a Search Query as a Routing Rule" on page 22
- "Saving a Search Query as a Retention Policy" on page 22

Saving a Search Query as a Search Template

1 Perform and refine a search until you are satisfied with the search results.

For more information, see "Refining Search Results" on page 17 .

2 Click **Save as**, and then click **Save search**.

3 Specify a unique name for the search and provide an optional description.

4 Specify the following information in the **Default Parameters** section:

Data sources: Displays the number of servers that Change Guardian will search for events. This option is useful if data federation is enabled. To select the data sources you want to search, click **selected data sources**, then select the data sources.

Email to: To e-mail the report template to others, specify the e-mail address. To send the report template to more than one person, specify multiple e-mail addresses separated by a comma.

Result limit: Specify the number of results to be stored in the search template. By default, 1000 results are stored in a report template.

5 Click **Save**.

Saving a Search Query as a Filter

You can save your search queries as filters for future use so you can perform a search using the saved filters rather than specifying the query manually every time.

To save a search query as a filter:

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

For more information, see "Refining Search Results" on page 17.

2 (Conditional) If you are using Change Guardian with traditional storage, click **Save as**, then click **Save search as filter**.

3 Specify a unique name for the filter and an optional description.

4 In the drop-down list, select one of the following options to specify the access for this filter:

- **Private:** Allows you to make this filter private. Other users cannot view or access this filter.
- **Public:** Allows you to share this filter with all users.
- **Users in same role:** Allows you to share this filter with users who have the same role as yours.
- **Users in selected roles:** Allows you to share this filter with users in specific roles. If you select this option, a blank field is displayed where you can specify the roles. As you type the role name, a list of roles is displayed.

  Select one or more roles.

  NOTE: This option is available only for users in the administrator role.

5 Click **Save**.

The saved filter is listed in the Filters panel.

Saving a Search Query as a Report Template

You can save the search query as a search report.

NOTE: You must have the Manage Reports permission to save the search query as a report template.

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

For more information, see "Refining Search Results" on page 17.

2 When you are satisfied with the search results, click **Save as**, then click **Save search as report**.

3 Specify the following parameters:

Parameter	Description
Report name	Specify a unique name for the report. The name should not exceed 200 characters.
Based on	Select the base report from which you want to create the report. You can view a sample report by clicking the **View Sample** button.
Description	The description is automatically displayed based on the report that is selected and you can edit the description.
Criteria	Criteria is automatically populated based on the report selected and is not editable.
Additional criteria	Specify additional search criteria to the existing criteria. To build a new criteria on your own, click **Edit Criteria**. To build a new criteria from available system objects containing criteria, click **Add Criteria**. The criteria that you add here is appended to the existing criteria.
Data sources	Select the source machines on which the reports can be run by clicking the **selected data sources** link. You can select data sources only if your Change Guardian is configured for data federation. For more information, see Configuring Data Federation in the "*Change Guardian Installation and Administration Guide*".

Parameter	Description
Additional Criteria	Specify additional criteria to refine the results. The criteria that you specify here can be edited while scheduling the report. If you specify **Criteria name**, the name is displayed at the end of the report results. **NOTE:** This parameter is not available for all reports.
Time Zone	Specify the time zone with which you want to populate the report. When you schedule the report, the time zone that you specify here is displayed in the report data. For example, if the Time Zone is set to US/Pacific-New time, the report data displays the selected time zone. By default, it displays the time zone that is set in the client system. **NOTE:** This parameter is not available for all reports.
Date Range	If the report includes time period parameters, choose the date range. All time periods are based on the local time for the browser. The **From Date** and the `To Date` automatically change to reflect the option you selected. ◆ **Current Day:** Shows events from midnight of the current day until 11:59:00 PM of the current day. If the current time is 8:00:00 AM, the report shows 8 hours of data. ◆ **Previous Day:** Shows events from midnight yesterday until 11:59:00 PM yesterday. ◆ **Week To Date:** Shows events from midnight Sunday of the current week until the end of the selected day. ◆ **Previous Week:** Shows events for the last seven days. ◆ **Month to Date:** Shows events from midnight the first day of the current month until the end of the selected day. ◆ **Previous Month:** Shows events for a month, from midnight of the first day of the previous month until 11:59:00 PM. of the last day of the previous month. ◆ **Custom Date Range:** Shows events for a period whose start and end date are chosen. If you select **Custom Date Range**, set the start date (**From Date**) and the end date (**To Date**) for the report.
From Date	Lets you set the from date.
To Date	Lets you set the to date.
Event Name	Name of the event. Default value is *
Severity	0 1 All
Email to	Specify an e-mail address in the **Email to** field. If you want to mail the report to more than one user, separate the e-mail addresses with a comma.

Parameter	Description
Result limit	Specify the number of results to be displayed or stored when you run or schedule the report. By default, 1000 results are stored. If you specify a value in **Group By** field, the result limit is based on grouping.

4 Click **Save** to save the search as report definition.

You can see the saved report definition in the **Reports and Searches** panel in the Administration Console. To view the reports, see "Working with Reports" on page 47.

Saving a Search Query as a Routing Rule

You must be in the administrator role to save the search query as a routing rule.

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

For more information, "Refining Search Results" on page 17.

2 When you are satisfied with the search results, click **Save as**, then click **Save search as routing rule**.

3 Specify a name for the rule.

4 (Conditional) To associate one or more tags to the events, click **Select tag**, select the desired tags, then click **Set**.

5 Select where you want to route the events to:

- **All:** Events are routed to all Change Guardian services, including Correlation and Security Intelligence.
- **Event store only:** Events are sent directly to the event store, and are not displayed in Event Views and the search results page.
- **None (drop):** Events are dropped or ignored, and are not sent to any Change Guardian service.

6 Select one or more actions to be performed on each event that meets the search criteria. Click the plus and minus icons to add and remove actions.

7 Click **Save**.

Saving a Search Query as a Retention Policy

You must be in the administrator role to save the search query as a retention policy.

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

For more information, see "Searching Events" on page 13 and "Refining Search Results" on page 17.

2 When you are satisfied with the search results, click **Save as**, then click **Save search as retention policy**.

3 Specify a name for the retention policy.

4 In the **Keep at least** field, specify the minimum number of days to retain the events in the system. The value must be a valid positive integer.

5 (Optional) In the **Keep at most** field, specify the maximum number of days for which the events should be retained in the system.

The value must be a valid positive integer and must be greater than or equal to the **Keep at least** value. If no value is specified, the system retains the events in the system until the space is available in primary storage.

6 Click **Save**.

The newly created policy is displayed in the data retention table. For more information on retention policies, see Configuring Data Federation in the Change Guardian Installation and Administration Guide.

Exporting the Search Results to a File

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

For more information,

2 In the search results, select the events you want to export to a file.

3 Click **Event operations** > **Export to file.**

4 Specify the following information:

File Name: Specify a name for the file to which you want to export the search results.

Event Limit: Specify the maximum number of events to be saved. The event limit must be less than the number of events you selected and the maximum event limit is 200000.

All the search results are written into a `.csv` file. These files are then compressed into a `.zip` file for downloading.

5 (Optional) You can remove the event fields that you do not want to export to the file. Click **Choose Fields**, then clear the selections for the fields that you do not want to export to the file.

By default, the null fields are excluded and not exported to file.

6 Click **Export** to export the search result to a file.

A download file dialog box is displayed with an option to open or save the `.zip` file.

7 Select the desired option, then click **OK**.

Filtering Events

The Filters feature in Change Guardian allows you to customize the event search and prevent data overload. You can save a search query as a filter and reuse it as required, so that you can perform a search by selecting the filter rather than specifying the query manually every time.

Following sections provide information about configuring filters.

- “Creating Filters” on page 24
- “Sample Filters” on page 27
- “Viewing Events by Using Filters” on page 29
- “Managing Filters” on page 29

You can reuse filters while using or configuring Change Guardian features, such as:

- Configuring Data Synchronization
- Configuring a Data Retention policy.
- Configuring the data visibility settings for a role.
- Creating dashboards.

- Configuring event routing rules.
- Viewing real-time events in Event Views.

Change Guardian provides a list of filters by default. You can also create your own filters. To view the Filters available in Change Guardian, click **Filters** in the Administration Console on the left navigation panel.

- **My Filters:** Lists the default filters and the filters you created.
- **Shared Filters:** Lists the filters that other users have shared with you.

Creating Filters

Filter criteria are simple math expressions and simple evaluations. Filters work on selection sets by matching events against the specified criteria. If the match is TRUE, the event is displayed in real-time views or search results, or passed to other functions. If the match is FALSE, the event is blocked. The filter criteria is your search query.

For example, consider a search query that is written as follows:

```
(sip:"10.0.0.1")
```

Events whose source IP address is 10.0.0.1 are included in the filter.

You must use the event field ID to represent an event name. Click the **Tips** on the top right of the Administration Console for a list of event field names and their IDs.

Following sections provide information about creating filters.

- "Building a New Criteria" on page 24
- "Selecting an Existing Criteria" on page 26
- "Creating a Filter" on page 26

Building a New Criteria

The Build criteria interface provides a list of parameters required to build filter criteria ranging from simple to complex. You can either select the parameters, or you can manually specify the filter criteria.

The Build Criteria dialog box includes the following elements:

Table 3-1 *Build Criteria Dialog Box Elements*

Element	Description
Criteria	If you select **Structured**, this field displays the criteria formed by the parameters you select. You cannot modify or specify the filter criteria. If you select **Free-form**, you can manually specify the filter criteria.
Structured	Allows you to select the various parameters to build the filter criteria.

Element	Description
Free-form	Allows you to manually specify the filter criteria rather than selecting from the available parameters. The search criteria is based on the standard Lucene syntax with some Change Guardian extensions. If this option is selected, the following elements are not displayed: ◆ Event fields ◆ Criteria fields ◆ Field details
Exclude system events	Select this option to exclude Change Guardian internal events such as audit events and performance events from the search results.
Event fields	Displays a categorized list of possible event fields you can add to the filter criteria. You can expand each category to display the set of fields in that category. If you know the name of the field you want, specify the name in the **Search** field. The event category list will adjust to present only matching fields. For more information on event fields, click **Tips** located at the top right of the Administration Console.
Criteria fields	Lists a set of overlay criteria that you can use on top of per-field searches. The following fields are displayed by default: ◆ **All data:** Performs a search across all event fields. ◆ **Tags:** Events can be tagged in various ways to help identify relationships between events. Queries that include a “Tags” search will look at the event tags (rv145) for matches. ◆ **Taxonomy:** Events are also classified using a number of taxonomic categories for the action, outcome, and so on. Queries that include a “Taxonomy” search will search for specific classes of events.
Field details	The fields in this section vary depending on the event or criteria fields you select. For example: ◆ For tokenized fields, you can specify the words that you want to include or exclude in the filter criteria. For information on the tokenized and non-tokenized fields, click **Tips** located at the top right of the Administration Console. ◆ For non-tokenized fields, you can specify a value or a range of values. ◆ For taxonomy fields, specific taxonomy options are displayed. ◆ For date attributes, a date-time calendar is displayed as you type the date. You can select a date. ◆ For fields that contain internal Change Guardian UUIDs, such as the CollectorID field, the corresponding Change Guardian object names are displayed and can be selected.
Condition: AND OR	Allows you to specify the AND or OR condition between the criteria fields. These options are available when you add additional event criteria to the criteria fields.

Selecting an Existing Criteria

You can create a filter by using existing criteria from the predefined criteria list. The filter can be based on recent criteria, tags, or existing filters.

- **Show only recent criteria:** Select a search criterion from the recent search history. The search history displays a maximum of 15 search expressions. Select the criteria, click **Show only recent criteria**, and then click **Add**.
- **Show only tags:** You can search events that have a particular tag. Click **Show only tags** to list the tags in the system. Select the tags, and then click **Add**.
- **Show only filters:** You can reuse existing filters to perform a new search. Click **Show only filters** to list the existing filters. Select the filter on which you want to perform the search, and then click **Add**.

You can combine multiple criteria, tags, or filters by using the **And** or **Or** condition. After adding the criteria, you can test the filter by clicking **Test Filter**.

Creating a Filter

You can create filters either by building a new filter criteria or by saving a search query as a filter.

While creating a filter, you can specify whether you want to share a filter with other users. You must have the **Share Search Filters** permission to share filters with everyone or with users in the same role as yours. If you are a user in the administrator role, you can share filters with users in a different role.

Creating a Filter by Using the Build Criteria Dialog

1. Log in to the Administration Console.

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

   IP_Address/DNS_Change Guardian_server is the IP address or DNS name of the Change Guardian or server and *8443* is the default port for the Change Guardian server.
2. In the navigation panel, click **Filters** > **Create a filter**.
3. Select one of the following methods to create a filter criteria:
   - To build the filter criteria by selecting parameters, make sure that **Structured** is selected, select the parameters, then continue with Step 4.

     For information on these parameters, see Table 3-1, “Build Criteria Dialog Box Elements,” on page 24.
   - To manually specify the filter criteria rather than selecting the listed parameters, select **Free-form**. In the **Criteria** field, specify the filter criteria, then continue with Step 4.

     For information about the syntax for the criteria, see “Building a New Criteria” on page 24.
4. (Conditional) If you do not want to include Change Guardian internal events in the search, select **Exclude system events**.
5. Click **Search** to search events according to the specified filter criteria.

   By default, the search is performed on events that were generated within the last 1 hour.
6. Review the search results to verify that the filter is retrieving the expected events.
7. (Optional) You can modify the search query by selecting one or more event field values from the search results, or you can click **Edit search filter**, then make necessary changes.

8 When you are satisfied with the search results, click , then click **Save as Filter**.

9 Specify a name for the filter and an optional description.

10 In the **Sharing** drop-down list, select one of the following options to specify the access for this filter:

- **Private:** Allows you to make this filter private. Other users cannot view or access this filter.
- **Public:** Allows you to share this filter with all users.
- **Users in same role:** Allows you to share this filter with users who have the same role as yours.
- **Users in selected roles:** Allows you to share this filter with users in specific roles. If you select this option, a blank field is displayed where you can specify the roles. As you type the role name, a list of roles is displayed.

  Select one or more roles.

  NOTE: This option is available only for users in the administrator role or users with the **Share search filters** permission.

11 Click **Save**.

Creating a Filter by Using a Search Query

You can save a search query as a filter and use this filter to perform searches when required rather than specifying the search query again. For more information about creating a filter by using a search query, see "Saving a Search Query as a Filter" on page 19.

Sample Filters

This section lists a few examples on how you can create filters.

- "View Events of Severity 3 to 5 from a System in China" on page 27
- "Determine if User "Bob Smith" Tried to Log In after His Account was Disabled" on page 28
- "View Events from Two Subnets and Share the Filter with Network Administrators" on page 28
- "Find all Events that Include the Words "database" and "service," and exclude "test"" on page 29

View Events of Severity 3 to 5 from a System in China

- Click **Build Criteria** > **Event fields**, select **SourceHostCountry**.
- The name should match any string that contains the name "China." For example, "ChinaBeijing." Specify `china*` in the **Value** field.
- The severity of the events must be 3 to 5:
  - In **Event fields**, select **Severity**.
  - In the **Values that range from** field, specify 3 TO 5.

NOTE: If you are familiar with the search query syntax, you can directly specify the query in the **Criteria** field as follows:

```
(rv29:china*) AND (sev:[3 TO 5])
```

Click **Search** to view events that match the specified criteria.

Determine if User “Bob Smith” Tried to Log In after His Account was Disabled

- Click **Build Criteria** > **Event fields**, select the following:
  - **InitiatorUserName**
  - **TargetUserName**
  - **EffectiveUserName**
- Select the **OR** condition.
- Specify `"Bob Smith"` in the **Value** field.
- To determine if the user has logged in, or tried to log in, select **Taxonomy** in **Criteria fields.**

  NOTE: You can also select the appropriate event fields if you are familiar with the values to be specified for the event fields. Taxonomy is a classification of events where events of similar type are grouped together. It helps you search events based on the taxonomy classification rather than you specifying the specific event names and their values.

- In the **Field details**, select the following:
  - From the **Class** drop-down list, select **User Session Events**.
  - From the **Identifier** drop-down list, select **Create**.
  - For **Outcome**, select **Success**, then select **Failure**.

NOTE: If you are familiar with the search query syntax, you can directly specify the query in the **Criteria** field as follows:

```
(xdasclass:2 AND xdasid:0 AND (xdasoutcome:0 OR xdasoutcome:1)) AND (iufname:"Bob Smith")
```

Click **Search** to view the events that match the specified criteria.

View Events from Two Subnets and Share the Filter with Network Administrators

- Select subnets:
  - Click **Build Criteria** > **Event fields**, select **SourceIP**.
  - In **Field details** > **Value**, specify the subnet, for example, 172.17.0.0/16.
  - Repeat the above two steps to specify another subnet.
- The events must be from either of the subnets. Therefore, select **OR** as the condition.
- Click **Search** to view events that match the specified criteria.
- The filter must be shared with network administrators:
  - In the search results panel, click , then click **Save as new filter**.
  - Specify an intuitive name and an optional description.
  - From the drop-down list, select **Share with roles**, then select **Network Administrator**.
- Click **Save**.

Find all Events that Include the Words “database” and “service,” and exclude “test”

- Click **Build Criteria** > **Criteria fields**, select **All data**.
- You want to find events that include words “database” and “service,” and exclude “test.” Therefore, in **Field details**, specify the following:
  - In the **All of these words** field, specify `database service`.
  - In the **Exclude these words** field, specify `test`.

NOTE: If you are familiar with the search query syntax, you can directly specify the query in the **Criteria** field as follows:

```
_data:(database AND service) NOT _data:test
```

The `_data` field allows you to search for words that might appear in any event field.

Click **Search** to view the events that match the specified criteria.

Viewing Events by Using Filters

You can use filters to view events either by selecting the desired filter in the **Filters** panel or by using the **Filter** icon in the search results panel. For more information, see “Searching Events” on page 13.

Managing Filters

You can edit and delete only the filters that you created. The default filters and the filters that other users have shared with you cannot be edited or deleted.

Tagging Events

Tags are user-defined values that can be used to logically group data collection objects such as event routing rules, report templates, and report results. Tags help you to filter object lists for the data collection objects and also to augment incoming data. You can search for events, report templates, and report definitions that are tagged with a particular tag.

You can associate objects with more than one tag. You can, for example, create tags related to regulations (PCI) or compromised systems or network infrastructure such as routers, switches, and firewalls. Some organizations need to define data retention or data viewing policies based on the geographic location, so tags can be used to tag event sources based on different locations.

The **Tag** icon is available in various parts of the Administration Console which allows you to quickly add tags to the desired data collection objects such as report templates, and report results.

Following sections provide information about tagging:

- “Creating a Tag” on page 30
- “Viewing Tagged Events” on page 30
- “Managing Tags” on page 31
- “Performing Text Searches for Tags” on page 32

- “Deleting Tags” on page 32
- “Associating Tags with Objects” on page 32

Creating a Tag

To create a tag:

1. Log in to the Administration Console as a user in the Manage Tags role.

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

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

2. Select **Tags** in the navigation panel on the left or click the **Tag** icon in the appropriate data object interface to which you want to associate tags.
3. Click **Create**.
4. Specify a name for the tag.

   Tags have the following naming conventions, and a warning message is displayed if the name you specify does not comply with the following conventions:

   - Tag names should not be more than 20 characters.
   - There should not be any white space as part of the tag name.
   - A tag name is not case-sensitive. You cannot create two tags with identical names except for capitalization. For example, you cannot have the tag names `IDM` and `idm`, because both are perceived as the same name.
5. Specify an optional description for the tag.

   If the tag name is available, a message is displayed.

   If a tag with the same name already exists, a message is displayed indicating the name is not unique. You must specify a different name for the tag.
6. Click **Save**.

Viewing Tagged Events

You must have the appropriate permission to view events that are tagged with specific tags. For example, only users in the PCI Compliance Auditor role can view events that are tagged with at least one of the regulation-related tags such as PCI, SOX, HIPAA, NERC_CIP, FISMA, GLBA, NISPOM, JSOX, and ISO/IEC_27002:2005.

To view tagged events:

1. Log in to the Administration Console.
2. Do any of the following:
   - From the Tags panel, select the tag for which you want to view events, then select **Search**.
   - In the **Search** field, click the **Tag** icon, select the desired tags, then click **OK**. Click **Search**.
   - In the **Search** field, specify `rv145:<tagname>` or @<tagname> as the search criteria, then click **Search**.

Managing Tags

You can add and remove to favorites, view, edit, and sort tags

Following section provide information about managing tags.

- “Adding and Removing Tags from Favorites” on page 31
- “Sorting Tags” on page 31
- “Viewing and Modifying Tags” on page 31

Adding and Removing Tags from Favorites

You can add your frequently used tags to the Favorites section so that it is easier to locate them and associate them with objects. When a tag is added to the Favorites section, it is removed from the Other section.

To add or remove a tag from Favorites:

1. Log in to the Administration Console as a user in the Manage Tags role.
2. Select **Tags** in the navigation panel on the left.
3. To add or remove a tag from Favorites, select the tag, then click the **Favorites** icon.

Sorting Tags

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

To sort tags:

1. Log in to the Administration Console as a user in the Manage Tags role.
2. Select **Tags** in the navigation panel, then click **More**.
3. (Conditional) To sort the tags in the alphabetical order, select **Sort by Name**.
4. (Conditional) To sort the tags based on the number of objects associated with them, select **Sort by Count**.

The Tags are sorted according to the selection.

Viewing and Modifying Tags

You can modify only the description of a tag.The tag name cannot be modified because it might be used to tag events and other data collection objects, and it is not an accepted practice to modify events that are already stored. Therefore, to modify the name of a tag, you must create a new tag.

To view or modify a tag:

1. Log in to the Administration Console as a user in the Manage Tags role.
2. Select **Tags** in the navigation panel on the left.
3. Select the tag that you want to edit, and click the **Edit** icon.
4. Modify the description as necessary, then click **Save**.

Performing Text Searches for Tags

This option is useful when you want to look for a particular tag.

To search a tag:

1. Log in to the Administration Console as a user in the Manage Tags role.
2. Select **Tags** in the navigation panel on the left.
3. To search for a particular tag, specify the name or description of the tag or a keyword. To search for multiple tags, specify the tag names separated by the space character.

   The tag that matches the keyword is displayed.

Deleting Tags

To delete a tag:

1. Log in to the Administration Console as a user in the Manage Tags role.
2. Select **Tags** in the navigation panel on the left.
3. Select the tag that you want to delete, then click the **Delete** icon.

   The Change Guardian tag is a system tag that tags all Change Guardian internal events, and cannot be deleted.
4. Click **Delete** to confirm deletion.

Associating Tags with Objects

- "Associating Tags with Event Routing Rules" on page 32
- "Associating Tags with Report Results and Report Definitions" on page 32

You can associate tags with event routing rules, and reports and report templates. You can add more than one tag to a data collection object. However, the `rv145` field, which stores the tag value, can hold a maximum of 256 characters. Therefore, the maximum number of tags that you can associate with an object depends on the length of the tag name.

Associating Tags with Event Routing Rules

To associate tag with event routing rules:

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

Associating Tags with Report Results and Report Definitions

NOTE: When a tag is set on a report definition, the report results under the report definition inherit the tag by default. Inherited tags for a report result appear disabled in the Tag selector dialog box.

To associate a tag with reports:

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

Executing Actions

Users in the following roles can execute actions on events:

- Security Policy Administrator
- User

You need to configure the actions before executing actions on events.

To execute actions on events:

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

   For more information, "Performing a Search" on page 14.
2. In the search results, select the events on which you want to execute actions.
3. Click **Event operations** > **Show action panel**.
4. In the **Event Actions** panel > **Actions** drop-down, select the desired actions, then click **Execute**.

   The results of the actions are displayed in the **Results** field.

Viewing Vulnerabilities

You must have the View asset vulnerability data permission to view the Vulnerability data. You can view the vulnerabilities of the selected destination systems. To view the Vulnerability data, you must run the Vulnerability Collector and ensure that the Vulnerability scan information is being added to the Change Guardian database.

Vulnerabilities can be seen for the current time or for the event time.

- **View Vulnerabilities at current time:** This report queries the database for vulnerabilities that are active (effective) at the current date and time, and displays the relevant information.
- **View Vulnerabilities at time of event:** This report queries the database for vulnerabilities that were active (effective) at the date and time of the selected event, and displays the relevant events.

To view the Vulnerability report:

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

   For more information,
2. In the search results, select the events for which you want to view the Vulnerability data.

3 (Conditional) To view vulnerabilities at the current time, click **Event operations** > **View Vulnerabilities at current time**.

4 (Conditional) To view vulnerabilities at the time of the event, click **Event operations** > **View Vulnerabilities at time of event.**

4 Viewing Identity Data

This section provides information about integrating Change Guardian with Microsoft Active Directory (AD).

- “Performing a Search” on page 35
- “Viewing Profile Details” on page 36
- “Viewing Activities” on page 37
- “Searching and Viewing User Identities” on page 37

Performing a Search

The People Browser allows you to search for people to view what they have been doing. You can use the search box or click the arrow next to the search box for more options. As you start typing the information in the search field, the data is automatically displayed.

You can search for users by using the search box or by using the search fields.

- “Using the Search Box” on page 35
- “Using the Search Fields” on page 35

Using the Search Box

The search box automatically uses the following logic to interpret the text you enter:

- All letters and no spaces searches for the given name or surname.
- All letters and a space between letter groups searches for the given name and surname. The surname match is a starts-with, unless there is a trailing space.
- All letters with a comma in the middle is a match of the surname and given name. The given name match is starts-with unless there is a trailing space.
- Anything with a @ in it is a starts-with match for e-mail address.
- All digits, or letters and digits but no telephone punctuation characters is a starts-with match for workforce ID.
- Digits in addition to a leading +, and spaces, hyphens, periods, or parentheses is a starts-with match for a telephone number.
- Alphanumeric, or all numeric with no spaces, or all numbers with spaces is a starts-with match for the workforce ID.

Using the Search Fields

You can search for many values, including custom values, in the search fields. The following is a list of the fields you can search:

- Given Name
- Surname

- Telephone
- Email
- Position
- Department
- Office Location Code
- Workforce ID
- Vault Name
- Customer ID
- DN
- Custom Value Name
- Custom Value

Viewing Profile Details

After you have performed the search, (see "Performing a Search" on page 35), the user name, photo, position, department, e-mail, and telephone number are displayed.

Figure 4-1 *User Information Displayed*

You can also view detailed information about the user and all of the accounts that belong to this user.

You can use the clipboard functionality to copy the data of the user's profile and account information. Click the clipboard icon to the left of the user's photo and their information is now in the clipboard. You can paste this information into a text editor.

Viewing Activities

You can view the recent activity of a user through the People Browser.

- Authentication information
- Access events
- Permission changes

Searching and Viewing User Identities

The People Browser in Change Guardian allows you to search and view user profiles of identities in the Change Guardian database that have been synchronized with AD. In addition to information from the identity management system, the People Browser also shows recent user activity collected by Change Guardian.

5 Analyzing 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.

The following sections provide more information about alerts.

- "Analyzing Alerts in the Threat Response Dashboard and Alerts View" on page 39
- "Viewing Alerts in the Alert Dashboard" on page 41
- "Troubleshooting" on page 43

Analyzing Alerts in the Threat Response Dashboard and Alerts View

Change Guardian provides several ways to view alerts. The alerts you can view depend on the alert permissions applicable to your role and the tenancy of your role. For more information about permission to manage alerts, see Configuring Users and Roles in the *Change Guardian Installation and Administration Guide*.

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

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

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

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

NOTE: For users in the Operator role, the Threat Response dashboard is the main user interface for viewing and triaging alerts. Any user with permission to manage alerts can also use it. Users who wish to use alert views in the Administration Console, or do not have permission to view or manage alerts on the Threat Response dashboard, can use **Real-time Views** in Administration Console.

Alerts View In the Change Guardian Administration Console, alert views provide a graphical and tabular representation of alerts that match the specified alert criteria. Charts provide a summary of alerts and the table provides high-level information about individual alerts. Change Guardian provides some alert views, but you can also create your own alert views and customize the alert criteria as necessary.

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

As you monitor alerts, you can perform the following activities in the Threat Response Dashboard as well as the Alert View:

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

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

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

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

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

  - **Alert Fields:** Displays the alert fields that provide the following information:
    - who and what caused the alert.
    - the assets affected.
    - the taxonomic categories of the action that caused the alert, the outcome, and so on. For more information on taxonomy, see Sentinel Taxonomy.
  - **Trigger Events:** Displays the events that triggered the correlated event associated with the alert. You can determine the conditions that triggered the alert by examining the trigger events.
  - **Show history:** Displays the changes made to the alert, which helps you track any actions taken on the alert.
  - **Identities:** Displays the list of users involved in the alert. This information helps you to investigate the users involved in the alert and monitor their activities.

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

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

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

Viewing Alerts in the Alert Dashboard

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

Alert dashboards allow you to analyze and study common patterns in alerts, such as:

- Types of alerts
- Average time owners take to close alerts
- The correlation rule generating the maximum number of alerts
- Geographical origin of high-severity alerts
- Oldest open alerts
- Alerts that took the longest time to close

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

Overview Displays a time series chart that shows alerts generated in Change Guardian over time. You can inspect the time series charts for any spikes, which can indicate increase in attacks in your organization. You can drag and select the time period when the spike occurred to zoom into the alerts. As you select the specific time range, Change Guardian filters the dashboard for alerts in the selected time range. Also, you can find out the geographical locations from where the alerts originated. To view geographical locations from where the alerts originated, ensure that the `IpToCountry.csv` file is populated by using the `IP2Location Feed` plug-in.

Alert Load Provides information about the alerts at a granular level such as the following:

- Topmost alerts in your enterprise
- Alert distribution among top alert owners
- Total number of alerts in individual alert states
- Number of alerts received from each tenant
- Total number of alerts based on priority

Performance rows Provides statistical information about how efficiently alerts are investigated and closed based on priority, correlation rule, alert owners, and tenants.

Details Provides detailed alerts information such as the oldest open alerts, number of times the

duplicate alerts were rolled up, and all alert fields.

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

Viewing Alerts

To view the alert dashboard:

1. Log in to Change Guardian and click the **Alerts** dashboard.
2. Mouse over specific areas in the charts to view more information.
3. Select desired areas in the chart to Filter the alert data.
4. Click **Filtering** to remove the applied filters and go back to the unfiltered view.

   NOTE: As you select a specific area in the chart, Sentinel filters the alerts in rest of the charts and tables in the dashboard.

5. (Optional) You can customize the default view and save the dashboard. For information about customizing the dashboard.
6. (Conditional) To perform various operations on alerts such as closing an alert, assigning alerts to a user, and so on, see "Analyzing Alerts in the Threat Response Dashboard and Alerts View" on page 39.

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

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

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

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

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

Troubleshooting

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

Unable to View Alerts in the Dashboard and Alert Views

Issue: The alert dashboard and the charts in the alert view do not refresh or display new alerts. This issue could happen because of a corrupt alert index.

Workaround: Use the table in the alert view to see the newly generated alerts.

6 Managing Reports

Reports help you analyze events to assess your compliance regulatory requirements, security best practices, and corporate IT policies. You can use reports to demonstrate compliance and manage information security risk.

Reports emphasize the event data and help you analyze events such as user account visibility, detection of possible security violations, account compromises, network security problems, and any other undesired activities. By analyzing reports, you can configure appropriate correlation rules and actions to prevent any possible non-compliance activities and vulnerabilities.

Consider a scenario where you have an IT policy that states to remove access rights of all employees to information and information processing facilities upon termination of their employment. To view all deleted, and disabled user accounts, and revoked accesses, you can run a report that displays the desired information in a few clicks. You can also schedule the report to run periodically at specific intervals.

You can generate various types of Change Guardian reports for administration and auditing purposes.

The Administration Console includes a report for policy events. When you run the report, you can accept or customize the default options, including:

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

This chapter provides information about the following:

- “Creating Reports” on page 46
- “Scheduling Reports” on page 46
- “Working with Reports” on page 47
- “Rebranding Reports” on page 48

Creating Reports

A report is a template that is combined at run-time with a number of criteria, such as time parameters, user security filters, other filter criteria for the events to be displayed in the report. A single report may have numerous associated report results. Reports can range from a simple list of events to multiple graphs and tables.

You can manage the reports and report results in the **Reports and Searches** panel. To manage reports, you must have the **Manage Reports** permission.

You can also create new reports in the following ways:

- **Using an Existing Report:** You can create a new report based on existing reports. These reports include predefined criteria for the events to be displayed in the report. To create a new report, select the report based on which you want to create a new report, click **Create report**, and then add additional criteria to suit your requirements.

  NOTE: You can create new reports only from reports created by users in the same role as yours.

- **Using a Search Query:** You can save your search query as a new report.

  NOTE: While saving a search query, ensure that you select the relevant option under **Based On**. Each option under **Based On** creates filters in the search query.

Scheduling Reports

To view the report result, you must run the report. All reports have a sample report result. You can use the sample report to preview how the actual report result looks like when you run the report. To run the report, you must have the **Run reports** permission.

You can run the report immediately or schedule it to run periodically. Click the **Run** icon and specify the appropriate information to schedule a report. By default, Change Guardian saves the report in the PDF format.

Reports run asynchronously.Therefore, you can simultaneously perform other tasks in the Administration Console while the report generation is in progress. If the Change Guardian server is restarted while the report generation is still in progress, you can either cancel or reschedule report generation. If you reschedule the report, it runs with the same parameters that you used initially. If you schedule a report with a relative time setting, such as Week to Date, the time period for re-running the report is based on the current date and time and not the date and time when you initially scheduled the report.

NOTE: The report data in the PDF file will be different than the data in the reports that are run with the **Now** option. The report data in the PDF file are for the time range that you specified while scheduling a report definition. When you schedule a report definition with the **Now** option, the report includes events from midnight to the time you scheduled the report definition.

Scheduling Reports Across Change Guardian Servers

You can schedule reports on Change Guardian servers distributed across different geographic locations. For more information, see Data Federation in Change Guardian Administration Guide.

Saving Reports in the CSV Format

You can also save a report in the CSV format along with the existing PDF format. This requires additional configuration in the Change Guardian server. Only users in the administrator role can perform the additional configuration. For more information, see "Generating a Report in CSV Format" on page 47.

Generating a Report in CSV Format

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

To generate a report in CSV format:

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

   `vi obj-component.JasperReportingComponent.properties`
4. Edit the following entries:
   - `reporting.csv.enable=true`
   - `reporting.csv.outputdir=`*<the directory where the reports must be stored>*

   The `novell` user must have read/write permissions on the specified directory.
5. Restart the Change Guardian server.

When you generate a report, it is stored in the CSV format in the directory specified in the `reporting.csv.outputdir` attribute.

Working with Reports

The data that you view in reports depends on the security filter applied to your role. For example, if the security filter for your role is set to view events of severity 1 to 3, your report results will include only those events, although the report parameters allow severity 4 and 5 events also.

As you work with reports, you can perform several tasks including the following:

- **Finding Reports:** Change Guardian provides a large number of reports. You can use one of the following ways to easily find the reports you are interested in:
  - Using a particular keyword in the report name or description.
  - Using Tags.
  - Viewing reports belonging to a specific category: Scheduled or Unread.
- **Grouping:** To simplify report management as the number of reports grows over time, by default, Change Guardian groups the reports by **Category**.

  You can change the grouping to **None** if you want to list all your reports and searches under one heading. To change the grouping, click **More options**, select **Group by**, and then select the necessary option.
- **Tagging:** You can associate reports with existing tags. When a tag is set on a report, the report results associated with the report inherit the tag by default.

- **Marking reports and searches as Favorites:** You can mark the most frequently used reports and searches as Favorites to make them easier to find. You can also store them in folders to locate and manage them easily.
- **Drilling down into the reports to further analyze the data:** You can view events directly for a report without scheduling the report. The search results provide a preview of what to expect when you generate a report and the ability to investigate further. To view events for a report, click **Search Events**.
- **Sharing reports with other roles:** The **Share** functionality allows you to share reports with other roles and also control who can access your reports.

  For example, the out-of-the-box report templates are accessible to all Change Guardian users. Consider a scenario where you have several groups in your organization such as system administrators, database administrators. Because of the sensitivity of the audit data available in the report results when you run the out-of-the-box report templates, you may want to ensure that these administrators do not gain access to any unauthorized data. In such a scenario, you can restrict the report templates visibility only to you, to users in your role, or to users in selected roles.

  NOTE: Only users in the Administrator role can restrict the visibility of the out-of-the-box reports.

  For example, consider a scenario where there is a dedicated audit team in your organization whose primary job is to analyze and validate the accuracy of reports. You may want them to only view your reports but not modify or delete reports. In such a scenario, you can share your reports with the audit team. The audit team will only be able to view or run the reports depending on the permission they have. However, they will not be able to modify or delete reports.

  To share reports, you must have the **Share reports** permission. To share reports with users in other roles, you must have the **Manage roles and users** permission in addition to the **Share reports** permission. You can share only the reports that you create in the Administration Console. You cannot share reports that other users have shared with you. To share a report, select the report you want to share, click the **Share** icon, and select the relevant sharing option.

  The events in the report results that users, with whom you have shared reports, can view depend on the permission their role has. For example, if their role has permission to view only events of severity 4 and 5, the report results include only those events.

  If the user account of a report owner is deleted, reports that are set as **Private** are deleted. The ownership of all the shared reports is transferred to the admin user. If that report owner had shared any reports with you, you can no longer view those shared reports unless the admin user shares those reports with you.

Rebranding Reports

Change Guardian delivers an out-of-the-box Change Guardian white label report template. By customizing this template, you can rebrand the reports with your own header, footer, and logo. Only users in the administrator role can customize the Change Guardian white label report template.

To customize the template, perform the following:

1. In the **Reports and Searches** panel, select the Change Guardian White Label Template report definition, and then click Export.
2. Save the file to your local computer.
3. Create a new folder.
4. Extract the file contents to the new folder by using any ZIP extraction tool.

5 In the new folder, open the **resources** folder. In this folder, you can modify the following files:

- **Header/Footer.jrxml**: Contains the report layout descriptions. You can modify the layout of fields, text, or images in the header and footer, but you must ensure that the overall size of the header and footer does not change. You can manually edit the XML file or use iReport to modify them.
- **Header/Footer*.properties**: Contains the text in the layout file, which localized into various languages. You can modify the strings that appear in the header or footer by editing this file. Ensure that the new strings do no exceed the space allocated to them. For information about editing the `.properties` file, see Oracle Java documentation.
- **Logo.jpg**: Contains the logo that appears in the footer. You can replace this file with another image. Ensure that the size of the new image is exactly the same size of the existing image.

6 Use a ZIP tool to re-zip the modified report template.

7 In the **Reports and Searches** panel, click Import reports or searches, browse to this zip file, and then click Import.

NOTE: If the folder structure is different than the original ZIP file, the import process displays an error. Ensure that you do not modify the folder structure after making the changes.

---

8 Schedule any report definition and view the report to ensure that the changes are applied correctly.