



Extreme Networks Security Log Manager User Guide

Copyright © 2012–2015 All rights reserved.

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, please see:

www.extremenetworks.com/company/legal/trademarks/

Support

For product support, including documentation, visit: www.extremenetworks.com/documentation/

For information, contact:

Extreme Networks, Inc.

145 Rio Robles

San Jose, California 95134

USA

Table of Contents

About this Guide.....	6
Conventions.....	6
Providing Feedback to Us.....	7
Getting Help.....	8
Related Publications.....	8
Chapter 1: What's new for users in Log Manager V7.2.5.....	10
Chapter 2: Log Manager.....	11
Supported web browsers	11
User interface tabs.....	12
Extreme Security common procedures.....	14
Chapter 3: Dashboard management.....	19
Log activity.....	20
Most recent reports.....	20
System summary.....	20
Vulnerability Management items.....	21
System notification.....	21
Adding dashboard items.....	22
Using the dashboard to investigate log activity.....	22
Configuring charts.....	23
Removing dashboard items.....	23
Detaching a dashboard item.....	24
Renaming a dashboard	24
Deleting a dashboard.....	24
Managing system notifications.....	25
Adding search-based dashboard items to the Add Items list.....	25
Chapter 4: Log activity investigation.....	26
Log activity tab overview.....	26
Log activity monitoring.....	29
Viewing associated offenses.....	39
Modifying event mapping.....	39
PCAP data.....	40
Exporting events.....	42
Chapter 5: Asset Management overview.....	43
Asset data sources.....	44
Updates to asset data.....	44
Asset growth deviations.....	46
Example: Asset exclusion rules that are tuned to exclude IP addresses from the blacklist.....	51
Example: How configuration errors for log source extensions can cause asset growth deviations	52
Chapter 6: Chart management.....	53
Time series chart overview.....	54
Chart legends.....	55
Configuring charts.....	55

Chapter 7: Data searches.....	57
Searching for items that match your criteria.....	57
Saving search criteria.....	61
Scheduled search.....	62
Advanced search options.....	63
Quick filter search options.....	68
Using a subsearch to refine search results.....	69
Managing search results.....	70
Managing search groups.....	73
Chapter 8: Custom event properties.....	76
Required permissions.....	76
Custom property types.....	76
Creating a regex-based custom property.....	77
Creating a calculation-based custom property.....	78
Modifying a custom property.....	79
Copying a custom property.....	81
Deleting a custom property.....	81
Chapter 9: Rule management.....	82
Rule permission considerations.....	82
Rules overview.....	82
Viewing rules.....	84
Creating a custom rule.....	85
Creating an anomaly detection rule.....	86
Rule management tasks.....	87
Rule group management.....	88
Editing building blocks.....	91
Rule page parameters.....	91
Rules page toolbar.....	92
Rule Response page parameters.....	93
Chapter 10: Asset profiles.....	97
Vulnerabilities.....	97
Assets tab overview.....	98
Viewing an asset profile.....	100
Adding or editing an asset profile.....	102
Searching asset profiles.....	104
Saving asset search criteria.....	106
Asset search groups.....	106
Asset profile management tasks.....	108
Research asset vulnerabilities.....	110
Assets profile page parameters.....	112
Chapter 11: Report management.....	119
Reports tab overview.....	120
Creating custom reports.....	123
Report management tasks.....	127
Report groups.....	129
Appendix A: Glossary.....	133
A.....	134

B.....	134
C.....	134
D.....	135
E.....	135
F.....	135
G.....	136
H.....	136
I.....	136
K.....	137
L.....	137
M.....	137
N.....	138
O.....	138
P.....	138
Q.....	139
R.....	139
S.....	139
T.....	140
V.....	140
W.....	140
Index.....	141



About this Guide

The *Extreme Networks Security Log Manager Users Guide* provides information on managing Extreme SIEM including the Dashboard, Log Activity, and Reports tabs.

Intended audience

This guide is intended for all Extreme SIEM users responsible for investigating and managing network security. This guide assumes that you have Extreme SIEM access and a knowledge of your corporate network and networking technologies.

Statement of good security practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. Extreme Networks® systems, products and services are designed to be part of a lawful comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. EXTREME NETWORKS DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Note



Use of this Program may implicate various laws or regulations, including those related to privacy, data protection, employment, and electronic communications and storage. Extreme Networks Security Analytics may be used only for lawful purposes and in a lawful manner. Customer agrees to use this Program pursuant to, and assumes all responsibility for complying with, applicable laws, regulations and policies. Licensee represents that it will obtain or has obtained any consents, permissions, or licenses required to enable its lawful use of Extreme Networks Security Analytics.

Conventions

This section discusses the conventions used in this guide.

Text Conventions

The following tables list text conventions that are used throughout this guide.

Table 1: Notice Icons






Icon	Notice Type	Alerts you to...
	Tip	Helpful tips for using the product.
	Note	Important features or instructions.
	Caution	Risk of personal injury, system damage, or loss of data.
	Warning	Risk of severe personal injury.
	New	This command or section is new for this release.

Table 2: Text Conventions

Convention	Description
Screen displays	This typeface indicates command syntax, or represents information as it appears on the screen.
The words enter and type	When you see the word “enter” in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says “type.”
[Key] names	Key names are written with brackets, such as [Return] or [Esc]. If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press [Ctrl]+[Alt]+[Del]
Words in <i>italicized type</i>	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.

Terminology

When features, functionality, or operation is specific to a switch family, the family name is used. Explanations about features and operations that are the same across all product families simply refer to the product as the “switch.”

Providing Feedback to Us

We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

- Content errors or confusing or conflicting information.
- Ideas for improvements to our documentation so you can find the information you need faster.
- Broken links or usability issues.

If you would like to provide feedback to the Extreme Networks Information Development team about this document, please contact us using our short [online feedback form](#). You can also email us directly at InternalInfoDev@extremenetworks.com.

Getting Help

If you require assistance, contact Extreme Networks Global Technical Assistance Center using one of the following methods:

Web	www.extremenetworks.com/support
Phone	1-800-872-8440 (toll-free in U.S. and Canada) or 1-603-952-5000 For the Extreme Networks support phone number in your country: www.extremenetworks.com/support/contact
Email	support@extremenetworks.com To expedite your message, enter the product name or model number in the subject line.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number
- A description of the failure
- A description of any action(s) already taken to resolve the problem (for example, changing mode switches or rebooting the unit)
- The serial and revision numbers of all involved Extreme Networks products in the network
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load and frame size at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any previous Return Material Authorization (RMA) numbers

Related Publications

The Extreme Security product documentation listed below can be downloaded from <http://documentation.extremenetworks.com>.

Extreme Security Analytics Threat Protection

- *Extreme Networks Security API Reference Guide*
- *Extreme Networks Security Application Configuration Guide*
- *Extreme Networks Security Ariel Query Language Guide*
- *Extreme Networks Security DSM Configuration Guide*
- *Extreme Security DSM Configuration Guide Addendum*
- *Extreme Networks Security Hardware Guide*
- *Extreme Networks Security Installation Guide*
- *Extreme Networks Security Juniper NSM Plug-in User Guide*
- *Extreme Networks Security Log Manager Administration Guide*

- *Extreme Networks Security Log Sources User Guide*
- *Extreme Networks Security Managing Log Sources Guide*
- *Extreme Networks Security Offboard Storage Guide*
- *Extreme Security Release Notes*
- *Extreme Networks Security Risk Manager Adapter Configuration Guide*
- *Extreme Networks Security Risk Manager Getting Started Guide*
- *Extreme Networks Security Risk Manager Installation Guide*
- *Extreme Networks Security Risk Manager Migration Guide*
- *Extreme Networks Security Risk Manager User Guide*
- *Extreme Networks Security Troubleshooting System Notifications Guide*
- *Extreme Networks Security Upgrade Guide*
- *Extreme Networks Security Vulnerability Manager Release Notes*
- *Extreme Networks Security Vulnerability Manager User Guide*
- *Extreme Networks Security WinCollect User Guide*
- *Extreme Networks SIEM Administration Guide*
- *Extreme Networks SIEM Getting Started Guide*
- *Extreme Networks SIEM High Availability Guide*
- *Extreme Networks SIEM Troubleshooting Guide*
- *Extreme Networks SIEM Tuning Guide*
- *Extreme Networks SIEM Users Guide*
- *Migrating Extreme Security Log Manager to Extreme SIEM*


Extreme Security Threat Protection


- *Extreme Security Intrusion Prevention System Hardware Replacement Guide*
- *Extreme Security Threat Protection Release Notes*

1 What's new for users in Log Manager V7.2.5

Extreme Networks Security Log Manager V7.2.5 introduces reporting enhancements, new advanced search options, and more.

Reporting enhancements

You can share reports with groups of users. You can add a report to a report group that is shared with everyone or a group that is shared only with users who have specific user roles and security profiles.  [Learn more...](#)

You can set a classification for a report, such as confidential or internal only, which appears in the report header and footer. You can also add page numbers and create reports that are based on saved asset searches.  [Learn more...](#)

More advanced search options

Use the TEXT SEARCH operator to perform full text searches and find specific text in custom properties for events.  [Learn more...](#)

Modifying a custom rule keeps the state information for all rules

When you edit a custom rule and save the changes, only the rule that you are modifying and any rules that depend on that rule are affected. All state information, counters, and rule results for other rules are maintained. In previous releases, when you edited a custom rule, all rules and counters in the custom rule engine were reset. For example, if you were tracking a sequence of events, such as 5 failed logons followed by a successful logon, the count was reset when you modified and saved any rule.

For more information, see the [Rule text counter](http://www-01.ibm.com/support/docview.wss?crawler=1&uid=swg11V46111) APAR (<http://www-01.ibm.com/support/docview.wss?crawler=1&uid=swg11V46111>).

2 Log Manager

Supported web browsers

User interface tabs

Extreme Security common procedures

Extreme Networks Security Log Manager is a network security management platform that provides situational awareness and compliance support through security event correlation, analysis, and reporting.

Navigate the web-based application

When you use Log Manager, use the navigation options available in the user interface instead of your web browser **Back** button.

Supported web browsers

For the features in Extreme Networks Security Analytics products to work properly, you must use a supported web browser.

When you access the Extreme Security system, you are prompted for a user name and a password. The user name and password must be configured in advance by the administrator.

The following table lists the supported versions of web browsers.

Table 3: Supported web browsers for Extreme Security products

Web browser	Supported versions
Mozilla Firefox	17.0 Extended Support Release 24.0 Extended Support Release
32-bit Microsoft™ Internet Explorer, with document mode and browser mode enabled	9.0 10.0
Google Chrome	The current version as of the release date of the Extreme Networks Security Analytics version that you have installed.

Enabling document mode and browser mode in Internet Explorer

If you use Microsoft™ Internet Explorer to access Extreme Networks Security Analytics products, you must enable browser mode and document mode.

- 1 In your Internet Explorer web browser, press F12 to open the **Developer Tools** window.

- 2 Click **Browser Mode** and select the version of your web browser.
- 3 Click **Document Mode**.
 - For Internet Explorer V9.0, select **Internet Explorer 9 standards**.
 - For Internet Explorer V10.0, select **Internet Explorer 10 standards**.

User interface tabs

Functionality is divided into tabs. The **Dashboard** tab is displayed when you log in.

You can easily navigate the tabs to locate the data or functionality you require.

Dashboard tab

The **Dashboard** tab is the default tab that is displayed when you log in.

The **Dashboard** tab is the default tab that is displayed when you log in to Extreme Networks Security Log Manager. It provides a workspace environment that provides summary and detailed information on events occurring in your network.

Log activity tab

The **Log Activity** tab will allow you to investigate event logs being sent to Extreme Security in real-time, perform powerful searches, and view log activity by using configurable time-series charts.

The **Log Activity** tab will allow you to perform in-depth investigations on event data.

For more information, see [Log Activity investigation](#).

Assets tab

Extreme Security automatically discovers assets, servers, and hosts, operating on your network.

Asset profiles provide information about each known asset in your network, including identity information, if available, and what services are running on each asset. This profile data is used for correlation purposes to help reduce false positives.

For example, an attack tries to use a specific service that is running on a specific asset. In this situation, Extreme Security can determine whether the asset is vulnerable to this attack by correlating the attack to the asset profile. Using the **Assets** tab, you can view the learned assets or search for specific assets to view their profiles.

For more information, see [Asset management](#).

Reports tab

The **Reports** tab will allow you to create, distribute, and manage reports for any data within Extreme Security.

The Reports feature will allow you to create customized reports for operational and executive use. To create a report, you can combine information (such as, security or network) into a single report. You can also use preinstalled report templates that are included with Extreme Security.

The **Reports** tab also will allow you to brand your reports with customized logos. This customization is beneficial for distributing reports to different audiences.

For more information about reports, see [Reports management](#).

Vulnerability Manager tab

Vulnerability Manager is an Extreme Security component that you can purchase separately. You use a license key to enable Extreme Security Vulnerability Manager.

Extreme Security Vulnerability Manager is a network-scanning platform that provides awareness of the vulnerabilities that exist within the applications, systems, or devices on your network. After scans identify vulnerabilities, you can search and review vulnerability data, remediate vulnerabilities, and rerun scans to evaluate the new level of risk.

When Vulnerability Manager is enabled, you can perform vulnerability assessment tasks on the Vulnerabilities tab. From the Assets tab, you can run Vulnerability Manager scans on selected assets.

For more information, see the *Extreme Networks Security Vulnerability Manager User Guide*.

Admin tab

Administrators use the Admin tab to configure and manage the users, systems, networks, plug-ins, and components. Users with administration privileges can access the **Admin** tab.

The administration tools that administrators can access in the **Admin** tab are described in [Table 1](#).

Table 4: Administration management tools available in Extreme Security

Admin tool	Description
System Configuration	Configure system and user management options.
Data Sources	Configure log sources.
Remote Networks and Services Configuration	Configure remote networks and services groups.
Plug-ins	Access plug-in components, such as the Extreme Networks Security Risk Manager plug-in. This option is only displayed if there are plug-ins that are installed on your Console.
Deployment Editor	Manage the individual components of your Extreme Security deployment.

All configuration updates that you make in the **Admin** tab are saved to a staging area. When all changes are complete, you can deploy the configuration updates to the managed host in your deployment.

Extreme Security common procedures

Various controls on the Extreme Security user interface are common to most user interface tabs.

Information about these common procedures is described in the following sections.

Viewing messages

The **Messages** menu, which is on the upper right corner of the user interface, provides access to a window in which you can read and manage your system notifications.

For system notifications to show on the **Messages** window, the administrator must create a rule that is based on each notification message type and select the **Notify** check box in the **Custom Rules Wizard**.

The **Messages** menu indicates how many unread system notifications you have in your system. This indicator increments the number until you close system notifications. For each system notification, the **Messages** window provides a summary and the date stamp for when the system notification was created. You can hover your mouse pointer over a notification to view more detail. Using the functions on the **Messages** window, you can manage the system notifications.

System notifications are also available on the **Dashboard** tab and on an optional pop-up window that can be displayed on the lower left corner of the user interface. Actions that you perform in the **Messages** window are propagated to the **Dashboard** tab and the pop-up window. For example, if you close a system notification from the **Messages** window, the system notification is removed from all system notification displays.

For more information about Dashboard system notifications, see [System Notifications item](#).

The **Messages** window provides the following functions:

Table 5: Functions available in the Messages window

Function	Description
All	Click All to view all system notifications. This option is the default, therefore, you click All only if you selected another option and want to display all system notifications again.
Health	Click Health to view only system notifications that have a severity level of Health.
Errors	Click Errors to view only system notifications that have a severity level of Error.
Warnings	Click Warnings to view only the system notifications that have a severity level of Warning.
Information	Click Information to view only the system notifications that have a severity level of information.
Dismiss All	Click Dismiss All to close all system notifications from your system. If you filtered the list of system notifications by using the Health , Errors , Warnings , or Information icons, the text on the View All icon changes to one of the following options: <ul style="list-style-type: none"> Dismiss All Errors Dismiss All Health Dismiss All Warnings Dismiss All Warnings Dismiss All Info

Table 5: Functions available in the Messages window (continued)

Function	Description
View All	Click View All to view the system notification events in the Log Activity tab. If you filtered the list of system notifications by using the Health , Errors , Warnings , or Information icons, the text on the View All icon changes to one of the following options: <ul style="list-style-type: none"> • View All Errors • View All Health • View All Warnings • View All Info
Dismiss	Click the Dismiss icon beside a system notification to close the system notification from your system.

- 1 Log in to Extreme Security .
- 2 On the upper right corner of the user interface, click **Messages**.
- 3 On the **Messages** window, view the system notification details.
- 4 Optional. To refine the list of system notifications, click one of the following options:
 - **Errors**
 - **Warnings**
 - **Information**

- 5 Optional. To close system notifications, choose of the following options:

Option	Description
--------	-------------

Dismiss All	Click to close all system notifications.
--------------------	--

Dismiss	Click the Dismiss icon next to the system notification that you want to close.
----------------	---

- 6 Optional. To view the system notification details, hover your mouse pointer over the system notification.

Sorting results

You sort the results in tables by clicking a column heading. An arrow at the top of the column indicates the direction of the sort.

- 1 Log in to Extreme Security.
- 2 Click the column header once to sort the table in descending order; twice to sort the table in ascending order.

Refreshing and pausing the user interface

You can manually refresh, pause, and play the data that is displayed on tabs.

The **Log Activity** tab automatically refreshes every 60 seconds if you are viewing the tab in Last Interval (auto refresh) mode.

The timer, which is on the upper right corner of the interface, indicates the amount of time until the tab is automatically refreshed.

When you view the **Log Activity** tab in Real Time (streaming) or Last Minute (auto refresh) mode, you can use the **Pause** icon to pause the current display.

You can also pause the current display in the **Dashboard** tab. Clicking anywhere inside a dashboard item automatically pauses the tab. The timer flashes red to indicate that the current display is paused.

- 1 Log in to Extreme Security.
- 2 Click the tab that you want to view.
- 3 Choose one of the following options:

Option	Description
Refresh	Click Refresh , on the right corner of the tab, to refresh the tab.
Pause	Click to pause the display on the tab.
Play	Click to restart the timer after the timer is paused.

Investigate user names

You can right-click a user name to access more menu options. Use these options to view more information about the user name or IP address.

You can investigate user names when Extreme Networks Security Vulnerability Manager is purchased and licensed. For more information, see the *Extreme Networks Security Vulnerability Manager User Guide*.

When you right-click a user name, you can choose the following menu options.

Table 6: Menu options for user name investigation

Option	Description
View Assets	Displays current assets that are associated to the selected user name. For more information about viewing assets, see Asset management .
View User History	Displays all assets that are associated to the selected user name over the previous 24 hours.
View Events	Displays the events that are associated to the selected user name. For more information about the List of Events window, see Log activity monitoring .

For more information about customizing the right-click menu, see the *Administration Guide* for your product.

System time

The right corner of the Extreme Security user interface displays system time, which is the time on the console.

The console time synchronizes Extreme Security systems within the Extreme Security deployment. The console time is used to determine what time events were received from other devices for correct time synchronization correlation.

In a distributed deployment, the console might be in a different time zone from your desktop computer.

When you apply time-based filters and searches on the **Log Activity** tab, you must use the console system time to specify a time range.

Updating user preferences

You can set your user preference, such as locale, in the main Extreme SIEM user interface.

- 1 To access your user information, click **Preferences**.
- 2 Update your preferences.

Option	Description
Username	Displays your user name. You cannot edit this field.
Password	<p>The password must meet the following criteria:</p> <ul style="list-style-type: none"> • Minimum of 6 characters • Maximum of 255 characters • Contain at least 1 special character • Contain 1 uppercase character
Password (Confirm)	Password confirmation
Email Address	<p>The email address must meet the following requirements:</p> <ul style="list-style-type: none"> • Minimum of 10 characters • Maximum of 255 characters
Locale	<p>Extreme Security is available in the following languages: English, Simplified Chinese, Traditional Chinese, Japanese, Korean, French, German, Italian, Spanish, Russian, and Portuguese (Brazil).</p> <p>If you choose a different language, the user interface displays in English. Other associated cultural conventions, such as, character type, collation, format of date and time, currency unit are used.</p>
Enable Popup Notifications	Select this check box if you want to enable pop-up system notifications to be displayed on your user interface.

Resize columns

You can resize the columns on several tabs in Extreme Security.

Place the pointer of your mouse over the line that separates the columns and drag the edge of the column to the new location. You can also resize columns by double-clicking the line that separates the columns to automatically resize the column to the width of the largest field.



Note

Column resizing does not work in Microsoft™ Internet Explorer, Version 7.0 web browsers when tabs are displaying records in streaming mode.

Page size

Users with administrative privileges can configure the maximum number of results that display in the tables on various tabs in Extreme Security.

3 Dashboard management

Log activity
Most recent reports
System summary
Vulnerability Management items
System notification
Adding dashboard items
Using the dashboard to investigate log activity
Configuring charts
Removing dashboard items
Detaching a dashboard item
Renaming a dashboard
Deleting a dashboard
Managing system notifications
Adding search-based dashboard items to the Add Items list

The **Dashboard** tab is the default view when you log in.

It provides a workspace environment on which you can display your views of the data that is collected.

Use the Dashboard tab to monitor your security event behavior.

You can customize your dashboard. The content that is displayed on the **Dashboard** tab is user-specific. Changes that are made within a session affect only your system.

To customize your **Dashboard** tab, you can perform the following tasks:

- Add and remove dashboard items from your dashboards.
- Move and position items to meet your requirements. When you position items, each item is automatically resized in proportion to the dashboard.
- Add custom dashboard items that are based on any data.

For example, you can add a dashboard item that provides a time series graph or a bar chart that represents top 10 network activity.

To create custom items, you can create saved searches on the **Log Activity** tab and choose how you want the results that are represented in your dashboard. Each dashboard chart displays real-time up-to-the-minute data. Time series graphs on the dashboard refresh every 5 minutes.

Log activity

The **Log Activity** dashboard items will allow you to monitor and investigate events in real time.



Note

Hidden or closed events are not included in the values that are displayed in the **Dashboard** tab.

Table 7: Log activity items

Dashboard item	Description
Event Searches	<p>You can display a custom dashboard item that is based on saved search criteria from the Log Activity tab. Event search items are listed in the Add Item > Log Activity > Event Searches menu. The name of the event search item matches the name of the saved search criteria the item is based on.</p> <p>Extreme Security includes default saved search criteria that is preconfigured to display event search items on your Dashboard tab menu. You can add more event search dashboard items to your Dashboard tab menu. For more information, see Adding search-based dashboard items to the Add Items list.</p> <p>On a Log Activity dashboard item, search results display real time last-minute data on a chart. The supported chart types are time series, table, pie, and bar. The default chart type is bar. These charts are configurable.</p> <p>Time series charts are interactive. You can magnify and scan through a timeline to investigate log activity.</p>
Events By Severity	<p>The Events By Severity dashboard item displays the number of active events that are grouped by severity. This item will allow you to see the number of events that are received by the level of severity assigned. Severity indicates the amount of threat an offense source poses in relation to how prepared the destination is for the attack. The range of severity is 0 (low) to 10 (high). The supported chart types are Table, Pie, and Bar.</p>
Top Log Sources	<p>The Top Log Sources dashboard item displays the top 5 log sources that sent events to Extreme Security Log Manager within the last 5 minutes.</p> <p>The number of events that are sent from the specified log source is indicated in the pie chart. This item will allow you to view potential changes in behavior, for example, if a firewall log source that is typically not in the top 10 list now contributes to a large percentage of the overall message count, you should investigate this occurrence. The supported chart types are Table, Pie, and Bar.</p>

Most recent reports

The **Most Recent Reports** dashboard item displays the top recently generated reports.

The display provides the report title, the time, and date the report was generated, and the format of the report.

System summary

The **System Summary** dashboard item provides a high-level summary of activity within the past 24 hours.

Within the summary item, you can view the following information:

- **Current Events Per Second** - Displays the event rate per second.
- **New Events (Past 24 Hours)** - Displays the total number of new events that are received within the last 24 hours.

Vulnerability Management items

Vulnerability Management dashboard items are only displayed when Extreme Networks Security Vulnerability Manager is purchased and licensed.

For more information, see the *Extreme Networks Security Vulnerability Manager User Guide*.

You can display a custom dashboard item that is based on saved search criteria from the **Vulnerabilities** tab. Search items are listed in the **Add Item > Vulnerability Management > Vulnerability Searches** menu. The name of the search item matches the name of the saved search criteria the item is based on.

Extreme Security includes default saved search criteria that is preconfigured to display search items on your **Dashboard tab** menu. You can add more search dashboard items to your **Dashboard tab** menu.

The supported chart types are table, pie, and bar. The default chart type is bar. These charts are configurable.

System notification

The Systems Notification dashboard item displays event notifications that are received by your system.

For notifications to show in the **System Notification** dashboard item, the Administrator must create a rule that is based on each notification message type and select the **Notify** check box in the Custom Rules Wizard.

For more information about how to configure event notifications and create event rules, see the *Extreme Networks Security Log Manager Administration Guide*.

On the **System Notifications** dashboard item, you can view the following information:

- **Flag** - Displays a symbol to indicate severity level of the notification. Point to the symbol to view more detail about the severity level.
 - **Health** icon
 - **Information** icon (?)
 - **Error** icon (X)
 - **Warning** icon (!)
- **Created** - Displays the amount of time elapsed since the notification was created.
- **Description** - Displays information about the notification.
- **Dismiss icon (x)** - Will allow you to close a system notification.

You can point your mouse over a notification to view more details:

- **Host IP** - Displays the host IP address of the host that originated the notification.
- **Severity** - Displays the severity level of the incident that created this notification.
- **Low Level Category** - Displays the low-level category that is associated with the incident that generated this notification. For example: Service Disruption.

- **Payload** - Displays the payload content that is associated with the incident that generated this notification.
- **Created** - Displays the amount of time elapsed since the notification was created.

When you add the **System Notifications** dashboard item, system notifications can also display as pop-up notifications in the Extreme Security user interface. These pop-up notifications are displayed in the lower right corner of the user interface, regardless of the selected tab.

Pop-up notifications are only available for users with administrative permissions and are enabled by default. To disable pop-up notifications, select **User Preferences** and clear the **Enable Pop-up Notifications** check box.

In the **System Notifications** pop-up window, the number of notifications in the queue is highlighted. For example, if (1 - 12) is displayed in the header, the current notification is 1 of 12 notifications to be displayed.

The **system notification** pop-up window provides the following options:

- **Next icon (>)** - Displays the next notification message. For example, if the current notification message is 3 of 6, click the icon to view 4 of 6.
- **Close icon (X)** - Closes this notification pop-up window.
- **(details)** - Displays more information about this system notification.

Adding dashboard items

You can add multiple dashboard items to your Dashboard tab.

- 1 Click the **Dashboard** tab.
- 2 From the toolbar, click **Add Item**.
- 3 Select the item you want to add. See Available dashboard items.

Using the dashboard to investigate log activity

Search-based dashboard items provide a link to the **Log Activity** tab, allowing you to further investigate log activity.

To investigate flows from a **Log Activity** dashboard item:

- 1 Click the **View in Log Activity** link. The **Log Activity** tab is displayed, displaying results and two charts that match the parameters of your dashboard item.

The chart types that are displayed on the **Log activity** tab depend on which chart is configured in the dashboard item:

Chart type	Description
Bar, Pie, and Table	The Log Activity tab displays a bar chart, pie chart, and table of details.
Time Series	The Log Activity tab displays charts according to the following criteria: <ol style="list-style-type: none"> 1 If your time range is less than or equal to 1 hour, a time series chart, a bar chart, and a table of event details are displayed.

Chart type	Description
	2 If your time range is more than 1 hour, a time series chart is displayed and you are prompted to click Update Details. This action starts the search that populates the event details and generates the bar chart. When the search completes, the bar chart and table of event details are displayed.

Configuring charts

You can configure **Log Activity**, **Network Activity**, and **Connections** (if applicable) dashboard items to specify the chart type and how many data objects you want to view.

Parameter options.

Table 8: Configuring Charts

option	description
Value to Graph	From the list box, select the object type that you want to graph on the chart. Options include all normalized and custom event or flow parameters included in your search parameters.
Chart Type	From the list box, select the chart type that you want to view. Options include: <ol style="list-style-type: none"> Bar Chart - Displays data in a bar chart. This option is only available for grouped events. Pie Chart - Displays data in a pie chart. This option is only available for grouped events. Table - Displays data in a table. This option is only available for grouped events. Time Series - Displays an interactive line chart that represents the records that are matched by a specified time interval.
Display Top	From the list box, select the number of objects you want you view in the chart. Options include 5 and 10 . The default is 10 .
Capture Time Series Data	Select this check box to enable time series capture. When you select this check box, the chart feature begins to accumulate data for time series charts. By default, this option is disabled.
Time Range	From the list box, select the time range that you want to view.

Your custom chart configurations are retained, so that they are displayed as configured each time that you access the **Dashboard** tab.

Log Manager collects data so that when you perform a time series saved search, there is a cache of event or flow data available to display the data for the previous time period. Accumulated parameters are indicated by an asterisk (*) in the **Value to Graph** list box. If you select a value to graph that is not accumulated (no asterisk), time series data is not available.

- 1 Click the **Dashboard** tab.
- 2 From the **Show Dashboard** list box, select the dashboard that contains the item you want to customize.
- 3 On the header of the dashboard item you want to configure, click the **Settings** icon.
- 4 Configure the chart parameters that are described in Table 1.

Removing dashboard items

You can remove items from a dashboard and add the item again at any time.

When you remove an item from the dashboard, the item is not removed completely.

- 1 Click the **Dashboard** tab.
- 2 From the **Show Dashboard** list box, select the dashboard from which you want to remove an item.
- 3 On the dashboard item header, click the red [x] icon to remove the item from the dashboard.

Detaching a dashboard item

You can detach an item from your dashboard and display the item in a new window on your desktop system.

When you detach a dashboard item, the original dashboard item remains on the **Dashboard** tab, while a detached window with a duplicate dashboard item remains open and refreshes during scheduled intervals. If you close the Extreme Security application, the detached window remains open for monitoring and continues to refresh until you manually close the window or shut down your computer system.

- 1 Click the **Dashboard** tab.
- 2 From the **Show Dashboard** list box, select the dashboard from which you want to detach an item.
- 3 On the dashboard item header, click the green icon to detach the dashboard item and open it in separate window.

Renaming a dashboard

You can rename a dashboard and update the description.

- 1 Click the **Dashboard** tab.
- 2 From the **Show Dashboard** list box, select the dashboard that you want to edit.
- 3 On the toolbar, click the **Rename Dashboard** icon.
- 4 In the **Name** field, type a new name for the dashboard. The maximum length is 65 characters.
- 5 In the **Description** field, type a new description of the dashboard. The maximum length is 255 characters.
- 6 Click **OK**.

Deleting a dashboard

You can delete a dashboard.

After you delete a dashboard, the **Dashboard** tab refreshes and the first dashboard that is listed in the **Show Dashboard** list box is displayed. The dashboard that you deleted is no longer displayed in the **Show Dashboard** list box.

- 1 Click the **Dashboard** tab.
- 2 From the **Show Dashboard** list box, select the dashboard that you want to delete.
- 3 On the toolbar, click **Delete Dashboard**.
- 4 Click **Yes**.

Managing system notifications

You can specify the number of notifications that you want to display on your **System Notification** dashboard item and close system notifications after you read them.

Ensure the **System Notification** dashboard item is added to your dashboard.

- 1 On the System Notification dashboard item header, click the **Settings** icon.
- 2 From the **Display** list box, select the number of system notifications you want to view.
 - The options are **5**, **10** (default), **20**, **50**, and **All**.
 - To view all system notifications that are logged in the past 24 hours, click **All**.
- 3 To close a system notification, click the **Delete** icon.

Adding search-based dashboard items to the Add Items list

You can add search-based dashboard items to your **Add Items** menu.

To add an event dashboard item to the **Add Item** menu on the **Dashboard** tab, you must access the **Log Activity** tab to create search criteria that specifies that the search results can be displayed on the **Dashboard** tab. The search criteria must also specify that the results are grouped on a parameter.

- 1 Choose:
 - To add an event search dashboard item, click the **Log Activity** tab.
- 2 From the **Search** list box, choose one of the following options:
 - To create a search, select **New Search**.
 - To edit a saved search, select **Edit Search**.
- 3 Configure or edit your search parameters, as required.
 - On the Edit Search pane, select the **Include in my Dashboard** option.
 - On the Column Definition pane, select a column and click the **Add Column** icon to move the column to the **Group By** list.
- 4 Click **Filter**.
The search results are displayed.
- 5 Click **Save Criteria**. See Saving search criteria on the Offense tab
- 6 Click **OK**.
- 7 Verify that your saved search criteria successfully added the event or flow search dashboard item to the **Add Items** list
- 8 Click the **Dashboard** tab.
- 9 To verify an event search item, select **Add Item > Log Activity > Event Searches > Add Item**

4 Log activity investigation

Log activity tab overview
Log activity monitoring
Viewing associated offenses
Modifying event mapping
PCAP data
Exporting events

You can monitor and investigate events in real time or perform advanced searches.

Using the **Log Activity** tab, you can monitor and investigate log activity (events) in real time or perform advanced searches.

Log activity tab overview

An event is a record from a log source, such as a firewall or router device, that describes an action on a network or host.

You must have permission to view the **Log Activity** tab.

Log activity tab toolbar

You can access several options from the Log Activity toolbar

Using the toolbar, you can access the following options:

Table 9: Log Activity toolbar options

Option	Description
Search	Click Search to perform advanced searches on events. Options include: <ul style="list-style-type: none">• New Search - Select this option to create a new event search.• Edit Search - Select this option to select and edit an event search.• Manage Search Results - Select this option to view and manage search results.
Quick Searches	From this list box, you can run previously saved searches. Options are displayed in the Quick Searches list box only when you have saved search criteria that specifies the Include in my Quick Searches option.
Add Filter	Click Add Filter to add a filter to the current search results.
Save Criteria	Click Save Criteria to save the current search criteria.
Save Results	Click Save Results to save the current search results. This option is only displayed after a search is complete. This option is disabled in streaming mode.

Table 9: Log Activity toolbar options (continued)



Option	Description
Cancel	Click Cancel to cancel a search in progress. This option is disabled in streaming mode.
Rules	<p>The Rules option is only visible if you have permission to view rules. Click Rules to configure custom event rules. Options include:</p> <ul style="list-style-type: none"> • Rules - Select this option to view or create a rule. If you only have the permission to view rules, the summary page of the Rules wizard is displayed. If you have the permission to maintain custom rules, the Rules wizard is displayed and you can edit the rule. To enable the anomaly detection rule options (Add Threshold Rule, Add Behavioral Rule, and Add Anomaly Rule), you must save aggregated search criteria because the saved search criteria specifies the required parameters. <hr/> <div>  <div> <p>Note</p> <p>The anomaly detection rule options are only visible if you have the Log Activity > Maintain Custom Rules permission.</p> </div> </div> <hr/> <ul style="list-style-type: none"> • Add Threshold Rule - Select this option to create a threshold rule. A threshold rule tests event traffic for activity that exceeds a configured threshold. Thresholds can be based on any data that is collected Extreme Security. For example, if you create a threshold rule indicating that no more than 220 clients can log in to the server between 8 am and 5 pm, the rules generate an alert when the 221st client attempts to log in. <p>When you select the Add Threshold Rule option, the Rules wizard is displayed, prepopulated with the appropriate options for creating a threshold rule.</p>
Rules (continued)	<ul style="list-style-type: none"> • Add Behavioral Rule - Select this option to create a behavioral rule. A behavioral rule tests event traffic for abnormal activity, such as the existence of new or unknown traffic, which is traffic that suddenly ceases or a percentage change in the amount of time an object is active. For example, you can create a behavioral rule to compare the average volume of traffic for the last 5 minutes with the average volume of traffic over the last hour. If there is more than a 40% change, the rule generates a response. <p>When you select the Add Behavioral Rule option, the Rules wizard is displayed, prepopulated with the appropriate options for creating a behavioral rule.</p> <ul style="list-style-type: none"> • Add Anomaly Rule - Select this option to create an anomaly rule. An anomaly rule tests event traffic for abnormal activity, such as the existence of new or unknown traffic, which is traffic that suddenly ceases or a percentage change in the amount of time an object is active. For example, if an area of your network that never communicates with Asia starts communicating with hosts in that country, an anomaly rule generates an alert. <p>When you select the Add Anomaly Rule option, the Rules wizard is displayed, prepopulated with the appropriate options for creating an anomaly rule.</p>

Table 9: Log Activity toolbar options (continued)


Option	Description
Actions	<p>Click Actions to perform the following actions:</p> <ul style="list-style-type: none"> • Show All - Select this option to remove all filters on search criteria and display all unfiltered events. • Print - Select this option to print the events that are displayed on the page. • Export to XML > Visible Columns - Select this option to export only the columns that are visible on the Log Activity tab. This is the recommended option. See Exporting events. • Export to XML > Full Export (All Columns) - Select this option to export all event parameters. A full export can take an extended period of time to complete. See Exporting events. • Export to CSV > Visible Columns - Select this option to export only the columns that are visible on the Log Activity tab. This is the recommended option. See Exporting events. • Export to CSV > Full Export (All Columns) - Select this option to export all event parameters. A full export can take an extended period of time to complete. See Exporting events. • Delete - Select this option to delete a search result. See Managing event and flow search results. • Notify - Select this option to specify that you want a notification emailed to you on completion of the selected searches. This option is only enabled for searches in progress. <hr/> <div>  <p>Note The Print, Export to XML, and Export to CSV options are disabled in streaming mode and when viewing partial search results.</p> </div>
Search toolbar	<p>Advanced Search Select Advanced Search from the list box to enter an Ariel Query Language (AQL) search string to specify the fields that you want returned.</p> <p>Quick Filter Select Quick Filter from the list box to search payloads by using simple words or phrases.</p>

Right-click menu options

On the **Log Activity** tab, you can right-click an event to access more event filter information.

The right-click menu options are:

Table 10: Right-click menu options

Option	Description
Filter on	Select this option to filter on the selected event, depending on the selected parameter in the event.
More options:	Select this option to investigate an IP address or a user name. For more information about investigating an IP address, see Investigating IP addresses . For more information about investigating a user name, see Investigating user names .
	<hr/> <div>  <p>Note This option is not displayed in streaming mode.</p> </div>

Status bar

When streaming events, the status bar displays the average number of results that are received per second.

This is the number of results the Console successfully received from the Event processors. If this number is greater than 40 results per second, only 40 results are displayed. The remainder is accumulated in the result buffer. To view more status information, move your mouse pointer over the status bar.

When events are not being streamed, the status bar displays the number of search results that are currently displayed on the tab and the amount of time that is required to process the search results.

Log activity monitoring

By default, the **Log Activity** tab displays events in streaming mode, allowing you to view events in real time.

For more information about streaming mode, see [Viewing streaming events](#). You can specify a different time range to filter events by using the **View** list box.

If you previously configured saved search criteria as the default, the results of that search are automatically displayed when you access the **Log Activity** tab. For more information about saving search criteria, see [Saving event and flow search criteria](#).

Viewing streaming events

Streaming mode will enable you to view event data that enters your system. This mode provides you with a real-time view of your current event activity by displaying the last 50 events.

If you apply any filters on the **Log Activity** tab or in your search criteria before enabling streaming mode, the filters are maintained in streaming mode. However, streaming mode does not support searches that include grouped events. If you enable streaming mode on grouped events or grouped search criteria, the **Log Activity** tab displays the normalized events. See [Viewing normalized events](#).

When you want to select an event to view details or perform an action, you must pause streaming before you double-click an event. When the streaming is paused, the last 1,000 events are displayed.

- 1 Click the **Log Activity** tab.
- 2 From the **View** list box, select **Real Time (streaming)**.
For information about the toolbar options, see Table 4-1. For more information about the parameters that are displayed in streaming mode, see Table 4-7.
- 3 Optional. Pause or play the streaming events. Choose one of the following options:
 - To select an event record, click the **Pause** icon to pause streaming.
 - To restart streaming mode, click the **Play** icon.

Viewing normalized events

Events are collected in raw format, and then normalized for display on the **Log Activity** tab.

Normalization involves parsing raw event data and preparing the data to display readable information about the tab. When events are normalized, the system normalizes the names as well. Therefore, the name that is displayed on the **Log Activity** tab might not match the name that is displayed in the event.



Note

If you selected a time frame to display, a time series chart is displayed. For more information about using time series charts, see [Time series chart overview](#).

The **Log Activity** tab displays the following parameters when you view normalized events:

Table 11: Log Activity tab - Default (Normalized) parameters






Parameter	Description
Current* Filters	<p>The top of the table displays the details of the filters that are applied to the search results. To clear these filter values, click Clear Filter.</p> <div>  <p>Note This parameter is only displayed after you apply a filter.</p> </div>
View	From this list box, you can select the time range that you want to filter for.
Current Statistics	<p>When not in Real Time (streaming) or Last Minute (auto refresh) mode, current statistics are displayed, including:</p> <div>  <p>Note Click the arrow next to Current Statistics to display or hide the statistics</p> </div> <ul style="list-style-type: none"> • Total Results - Specifies the total number of results that matched your search criteria. • Data Files Searched - Specifies the total number of data files searched during the specified time span. • Compressed Data Files Searched - Specifies the total number of compressed data files searched within the specified time span. • Index File Count - Specifies the total number of index files searched during the specified time span. • Duration - Specifies the duration of the search. <div>  <p>Note Current statistics are useful for troubleshooting. When you contact Customer Support to troubleshoot events, you might be asked to supply current statistical information.</p> </div>
Charts	<p>Displays configurable charts that represent the records that are matched by the time interval and grouping option. Click Hide Charts if you want to remove the charts from your display. The charts are only displayed after you select a time frame of Last Interval (auto refresh) or above, and a grouping option to display. For more information about configuring charts, see Chart management.</p> <div>  <p>Note If you use Mozilla Firefox as your browser and an ad blocker browser extension is installed, charts do not display. To displayed charts, you must remove the ad blocker browser extension. For more information, see your browser documentation.</p> </div>

Table 11: Log Activity tab - Default (Normalized) parameters (continued)

Parameter	Description
Offenses icon	Click this icon to view details of the offense that is associated with this event. For more information, see Chart management .
	 Note Depending on your product, this icon is might not be available. You must have Extreme SIEM.
Start Time	Specifies the time of the first event, as reported to Extreme Security by the log source.
Event Name	Specifies the normalized name of the event.
Log Source	Specifies the log source that originated the event. If there are multiple log sources that are associated with this event, this field specifies the term Multiple and the number of log sources.
Event Count	Specifies the total number of events that are bundled in this normalized event. Events are bundled when many of the same type of event for the same source and destination IP address are detected within a short time.
Time	Specifies the date and time when Extreme Security received the event.
Low Level Category	Specifies the low-level category that is associated with this event. For more information about event categories, see the <i>Extreme Networks Security Log Manager Administration Guide</i> .
Source IP	Specifies the source IP address of the event.
Source Port	Specifies the source port of the event.
Destination IP	Specifies the destination IP address of the event.
Destination Port	Specifies the destination port of the event.
Username	Specifies the user name that is associated with this event. User names are often available in authentication-related events. For all other types of events where the user name is not available, this field specifies N/A.
Magnitude	Specifies the magnitude of this event. Variables include credibility, relevance, and severity. Point your mouse over the magnitude bar to display values and the calculated magnitude.





- 1 Click the **Log Activity** tab.
- 2 From the **Display** list box, select **Default (Normalized)**.
- 3 From the **View** list box, select the time frame that you want to display.
- 4 Click the **Pause** icon to pause streaming.
- 5 Double-click the event that you want to view in greater detail. For more information, see [Event details](#).

Viewing raw events

You can view raw event data, which is the unparsed event data from the log source.

When you view raw event data, the **Log Activity** tab provides the following parameters for each event.

Table 12: Raw Event parameters

Parameter	Description
Current* Filters	<p>The top of the table displays the details of the filters that are applied to the search results. To clear these filter values, click Clear Filter.</p> <hr/> <div>  <div> Note This parameter is only displayed after you apply a filter. </div> </div>
View	From this list box, you can select the time range that you want to filter for.
Current* Statistics	<p>When not in Real Time (streaming) or Last Minute (auto refresh) mode, current statistics are displayed, including:</p> <hr/> <div>  <div> Note Click the arrow next to Current Statistics to display or hide the statistics </div> </div> <ul style="list-style-type: none"> • Total Results - Specifies the total number of results that matched your search criteria. • Data Files Searched - Specifies the total number of data files searched during the specified time span. • Compressed Data Files Searched - Specifies the total number of compressed data files searched within the specified time span. • Index File Count - Specifies the total number of index files searched during the specified time span. • Duration - Specifies the duration of the search. <hr/> <div>  <div> Note Current* statistics are useful for troubleshooting. When you contact Customer Support to troubleshoot events, you might be asked to supply current statistical information. </div> </div>
Charts	<p>Displays configurable charts that represent the records that are matched by the time interval and grouping option. Click Hide Charts if you want to remove the charts from your display. The charts are only displayed after you select a time frame of Last Interval (auto refresh) or above, and a grouping option to display.</p> <hr/> <div>  <div> Note If you use Mozilla Firefox as your browser and an ad blocker browser extension is installed, charts do not display. To displayed charts, you must remove the ad blocker browser extension. For more information, see your browser documentation. </div> </div>
Start Time	Specifies the time of the first event, as reported to Extreme Security by the log source.
Log Source	Specifies the log source that originated the event. If there are multiple log sources that are associated with this event, this field specifies the term Multiple and the number of log sources.
Payload	Specifies the original event payload information in UTF-8 format.

- 1 Click the **Log Activity** tab.
- 2 From the **Display** list box, select **Raw Events**.
- 3 From the **View** list box, select the time frame that you want to display.
- 4 Double-click the event that you want to view in greater detail. See [Event details](#).

Viewing grouped events

Using the **Log Activity** tab, you can view events that are grouped by various options. From the **Display** list box, you can select the parameter by which you want to group events.

The Display list box is not displayed in streaming mode because streaming mode does not support grouped events. If you entered streaming mode by using non-grouped search criteria, this option is displayed.

The Display list box provides the following options:

Table 13: Grouped events options

Group option	Description
Low Level Category	Displays a summarized list of events that are grouped by the low-level category of the event.
Event Name	Displays a summarized list of events that are grouped by the normalized name of the event.
Destination IP	Displays a summarized list of events that are grouped by the destination IP address of the event.
Destination Port	Displays a summarized list of events that are grouped by the destination port address of the event.
Source IP	Displays a summarized list of events that are grouped by the source IP address of the event.
Custom Rule	Displays a summarized list of events that are grouped by the associated custom rule.
Username	Displays a summarized list of events that are grouped by the user name that is associated with the events.
Log Source	Displays a summarized list of events that are grouped by the log sources that sent the event to Extreme Security.
High Level Category	Displays a summarized list of events that are grouped by the high-level category of the event.
Network	Displays a summarized list of events that are grouped by the network that is associated with the event.
Source Port	Displays a summarized list of events that are grouped by the source port address of the event.

After you select an option from the **Display** list box, the column layout of the data depends on the chosen group option. Each row in the events table represents an event group. The **Log Activity** tab provides the following information for each event group

Table 14: Grouped event parameters

Parameter	Description
Grouping By	Specifies the parameter that the search is grouped on.
Current* Filters	The top of the table displays the details of the filter that is applied to the search results. To clear these filter values, click Clear Filter .
View	From the list box, select the time range that you want to filter for.

Table 14: Grouped event parameters (continued)





Parameter	Description
Current* Statistics	<p>When not in Real Time (streaming) or Last Minute (auto refresh) mode, current statistics are displayed, including:</p> <div>  <p>Note Click the arrow next to Current Statistics to display or hide the statistics.</p> </div> <ul style="list-style-type: none"> • Total Results - Specifies the total number of results that matched your search criteria. • Data Files Searched - Specifies the total number of data files searched during the specified time span. • Compressed Data Files Searched - Specifies the total number of compressed data files searched within the specified time span. • Index File Count - Specifies the total number of index files searched during the specified time span. • Duration - Specifies the duration of the search. <div>  <p>Note Current* statistics are useful for troubleshooting. When you contact Customer Support to troubleshoot events, you might be asked to supply current statistic information.</p> </div>
Charts	<p>Displays configurable charts that represent the records that are matched by the time interval and grouping option. Click Hide Charts if you want to remove the chart from your display. Each chart provides a legend, which is a visual reference to help you associate the chart objects to the parameters they represent. Using the legend feature, you can perform the following actions:</p> <ul style="list-style-type: none"> • Move your mouse pointer over a legend item to view more information about the parameters it represents. • Right-click the legend item to further investigate the item. • Click a legend item to hide the item in the chart. Click the legend item again to show the hidden item. You can also click the corresponding graph item to hide and show the item. • Click Legend if you want to remove the legend from your chart display. <div>  <p>Note The charts are only displayed after you select a time frame of Last Interval (auto refresh) or above, and a grouping option to display.</p> </div> <div>  <p>Note If you use Mozilla Firefox as your browser and an ad blocker browser extension is installed, charts do not display. To display charts, you must remove the ad blocker browser extension. For more information, see your browser documentation.</p> </div>
Source IP (Unique Count)	Specifies the source IP address that is associated with this event. If there are multiple IP addresses that are associated with this event, this field specifies the term Multiple and the number of IP addresses.
Destination IP (Unique Count)	Specifies the destination IP address that is associated with this event. If there are multiple IP addresses that are associated with this event, this field specifies the term Multiple and the number of IP addresses.

Table 14: Grouped event parameters (continued)

Parameter	Description
Destination Port (Unique Count)	Specifies the destination ports that are associated with this event. If there are multiple ports that are associated with this event, this field specifies the term Multiple and the number of ports.
Event Name	Specifies the normalized name of the event.
Log Source (Unique Count)	Specifies the log sources that sent the event to Extreme Security. If there are multiple log sources that are associated with this event, this field specifies the term Multiple and the number of log sources.
High Level Category (Unique Count)	Specifies the high-level category of this event. If there are multiple categories that are associated with this event, this field specifies the term Multiple and the number of categories. For more information about categories, see the <i>Extreme Networks Security Log Manager Administration Guide</i> .
Low Level Category (Unique Count)	Specifies the low-level category of this event. If there are multiple categories that are associated with this event, this field specifies the term Multiple and the number of categories.
Protocol (Unique Count)	Specifies the protocol ID associated with this event. If there are multiple protocols that are associated with this event, this field specifies the term Multiple and the number of protocol IDs.
Username (Unique Count)	Specifies the user name that is associated with this event, if available. If there are multiple user names that are associated with this event, this field specifies the term Multiple and the number of user names.
Magnitude (Maximum)	Specifies the maximum calculated magnitude for grouped events. Variables that are used to calculate magnitude include credibility, relevance, and severity. For more information about credibility, relevance, and severity, see the Glossary .
Event Count (Sum)	Specifies the total number of events that are bundled in this normalized event. Events are bundled when many of the same type of event for the same source and destination IP address are seen within a short time.
Count	Specifies the total number of normalized events in this event group.

- 1 Click the **Log Activity** tab.
- 2 From the **View** list box, select the time frame that you want to display.
- 3 From the Display list box, choose which parameter you want to group events on. See Table 2. The events groups are listed. For more information about the event group details. See Table 1.
- 4 To view the **List of Events** page for a group, double-click the event group that you want to investigate. The **List of Events** page does not retain chart configurations that you might have defined on the **Log Activity** tab. For more information about the **List of Events** page parameters, see Table 1.
- 5 To view the details of an event, double-click the event that you want to investigate. For more information about event details, see Table 2.

Event details

You can view a list of events in various modes, including streaming mode or in event groups. In, whichever mode you choose to view events, you can locate and view the details of a single event.

The event details page provides the following information:

Table 15: Event details

Parameter	Description
Event Name	Specifies the normalized name of the event.
Low Level Category	Specifies the low-level category of this event.
Event Description	Specifies a description of the event, if available.
Magnitude	Specifies the magnitude of this event. For more information about magnitude, see the Glossary .
Relevance	Specifies the relevance of this event. For more information about relevance, see the Glossary .
Severity	Specifies the severity of this event. For more information about severity, see the Glossary .
Credibility	Specifies the credibility of this event. For more information about credibility, see the Glossary .
Username	Specifies the user name that is associated with this event, if available.
Start Time	Specifies the time of the event was received from the log source.
Storage Time	Specifies the time that the event was stored in the Extreme Security database.
Log Source Time	Specifies the system time as reported by the log source in the event payload.
Source and Destination information	
Source IP	Specifies the source IP address of the event.
Destination IP	Specifies the destination IP address of the event.
Source Asset Name	Specifies the user-defined asset name of the event source. For more information about assets, see Asset management.
Destination Asset Name	Specifies the user-defined asset name of the event destination. For more information about assets, see Asset management.
Source Port	Specifies the source port of this event.
Destination Port	Specifies the destination port of this event.
Pre NAT Source IP	For a firewall or another device capable of Network Address Translation (NAT), this parameter specifies the source IP address before the NAT values were applied. NAT translates an IP address in one network to a different IP address in another network.
Pre NAT Destination IP	For a firewall or another device capable of NAT, this parameter specifies the destination IP address before the NAT values were applied.
Pre NAT Source Port	For a firewall or another device capable of NAT, this parameter specifies the source port before the NAT values were applied.
Pre NAT Destination Port	For a firewall or another device capable of NAT, this parameter specifies the destination port before the NAT values were applied.
Post NAT Source IP	For a firewall or another device capable of NAT, this parameter specifies the source IP address after the NAT values were applied.
Post NAT Destination IP	For a firewall or another device capable of NAT, this parameter specifies the destination IP address after the NAT values were applied.

Table 15: Event details (continued)

Parameter	Description
Post NAT Source Port	For a firewall or another device capable of NAT, this parameter specifies the source port after the NAT values were applied.
Post NAT Destination Port	For a firewall or another device capable of NAT, this parameter specifies the destination port after the NAT values were applied.
Post NAT Source Port	For a firewall or another device capable of NAT, this parameter specifies the source port after the NAT values were applied.
Post NAT Destination Port	For a firewall or another device capable of NAT, this parameter specifies the destination port after the NAT values were applied.
IPv6 Source	Specifies the source IPv6 address of the event.
IPv6 Destination	Specifies the destination IPv6 address of the event.
Source MAC	Specifies the source MAC address of the event.
Destination MAC	Specifies the destination MAC address of the event.
Payload information	
Payload	Specifies the payload content from the event. This field offers 3 tabs to view the payload: <ul style="list-style-type: none"> • Universal Transformation Format (UTF) - Click UTF. • Hexadecimal - Click HEX. • Base64 - Click Base64.
Additional information	
Protocol	Specifies the protocol that is associated with this event.
QID	Specifies the QID for this event. Each event has a unique QID. For more information about mapping a QID, see Modifying event mapping .
Log Source	Specifies the log source that sent the event to Extreme Security. If there are multiple log sources that are associated with this event, this field specifies the term Multiple and the number of log sources.
Event Count	Specifies the total number of events that are bundled in this normalized event. Events are bundled when many of the same type of event for the same source and destination IP address are seen within a short time.
Custom Rules	Specifies custom rules that match this event. .
Custom Rules Partially Matched	Specifies custom rules that partially match this event.
Annotations	Specifies the annotation for this event. Annotations are text descriptions that rules can automatically add to events as part of the rule response.
Identity information - Extreme Security collects identity information, if available, from log source messages. Identity information provides extra details about assets on your network. Log sources only generate identity information if the log message sent to Extreme Security contains an IP address and least one of the following items: User name or MAC address. Not all log sources generate identity information. For more information about identity and assets, see Asset management .	
Identity Username	Specifies the user name of the asset that is associated with this event.
Identity IP	Specifies the IP address of the asset that is associated with this event.

Table 15: Event details (continued)


Parameter	Description
Identity Net Bios Name	Specifies the Network Base Input/Output System (Net Bios) name of the asset that is associated with this event.
Identity Extended field	Specifies more information about the asset that is associated with this event. The content of this field is user-defined text and depends on the devices on your network that are available to provide identity information. Examples include: physical location of devices, relevant policies, network switch, and port names.
Has Identity (Flag)	Specifies True if Extreme Security has collected identify information for the asset that is associated with this event. For more information about which devices send identity information, see the <i>Extreme Networks Security DSM Configuration Guide</i> .
Identity Host Name	Specifies the host name of the asset that is associated with this event.
Identity MAC	Specifies the MAC address of the asset that is associated with this event.
Identity Group Name	Specifies the group name of the asset that is associated with this event.

Event details toolbar

The events details toolbar provides several functions for viewing events detail.

The **event details** toolbar provides the following functions:

Table 16: Event details toolbar

Return to Events List	Click Return to Events List to return to the list of events.
Map Event	Click Map Event to edit the event mapping. For more information, see Modifying event mapping .
False Positive	Click False Positive to tune Extreme Security to prevent false positive events from generating into offenses.
Extract Property	Click Extract Property to create a custom event property from the selected event.
Previous	Click Previous to view the previous event in the event list.
Next	Click Next to view the next event in the event list.
PCAP Data	<div>  <div> <p>Note</p> <p>This option is only displayed if your Extreme Security Console is configured to integrate with the Juniper JunOS Platform DSM. For more information about managing PCAP data, see Managing PCAP data.</p> </div> </div> <ul style="list-style-type: none"> • View PCAP Information - Select this option to view the PCAP information. For more information, see Viewing PCAP information. • Download PCAP File - Select this option to download the PCAP file to your desktop system. For more information, see Downloading the PCAP file to your desktop system.
Print	Click Print to print the event details.

Viewing associated offenses

From the Log Activity tab, you can view the offense that is associated with the event.

If an event matches a rule, an offense can be generated on the **Offenses** tab.

When you view an offense from the **Log Activity** tab, the offense might not display if the Magistrate has not yet saved the offense that is associated with the selected event to disk or the offense has been purged from the database. If this occurs, the system notifies you.

- 1 Click the **Log Activity** tab.
- 2 Optional. If you are viewing events in streaming mode, click the **Pause** icon to pause streaming.
- 3 Click the **Offense** icon beside the event you want to investigate.
- 4 View the associated offense.

Modifying event mapping

You can manually map a normalized or raw event to a high-level and low-level category (or QID).

This manual action is used to map unknown log source events to known Extreme Security events so that they can be categorized and processed appropriately.

For normalization purposes, Extreme Security automatically maps events from log sources to high- and low-level categories.

For more information about event categories, see the *Extreme Networks Security Log Manager Administration Guide*.

If events are received from log sources that the system is unable to categorize, then the events are categorized as unknown. These events occur for several reasons, including:

- **User-defined Events** - Some log sources, such as Snort, allows you to create user-defined events.
- **New Events or Older Events** - Vendor log sources might update their software with maintenance releases to support new events that Extreme Security might not support.



Note

The **Map Event** icon is disabled for events when the high-level category is SIM Audit or the log source type is Simple Object Access Protocol (SOAP).

- 1 Click the **Log Activity** tab.
- 2 Optional. If you are viewing events in streaming mode, click the **Pause** icon to pause streaming.
- 3 Double-click the event that you want to map.
- 4 Click **Map Event**.
- 5 If you know the QID that you want to map to this event, type the QID in the **Enter QID** field.
- 6 If you do not know the QID you want to map to this event, you can search for a particular QID:
 - a Choose one of the following options: **To search for a QID by category, select the high-level category from the High-Level Category list box. To search for a QID by category, select the low-level category from the Low-Level Category list box. To search for a QID by log source type, select a log source type from the Log Source Type list box. To search for a QID by name, type a name in the QID/Name field.**

- b Click **Search**.
 - c Select the **QID** you want to associate this event with.
- 7 Click **OK**.

PCAP data

If your Extreme Security Console is configured to integrate with the Juniper JunOS Platform DSM, then Packet Capture (PCAP) can be received, processed, data can be stored from a Juniper SRX-Series Services Gateway log source.

For more information about the Juniper JunOS Platform DSM, see the *Extreme Networks Security DSM Configuration Guide*.

Displaying the PCAP data column

The **PCAP Data** column is not displayed on the **Log Activity** tab by default. When you create search criteria, you must select the **PCAP Data** column in the Column Definition pane.

Before you can display PCAP data on the **Log Activity** tab, the Juniper SRX-Series Services Gateway log source must be configured with the PCAP Syslog Combination protocol. For more information about configuring log source protocols, see the *Extreme Networks Security Managing Log Sources Guide*.

When you perform a search that includes the **PCAP Data** column, an icon is displayed in the **PCAP Data** column of the search results if PCAP data is available for an event. Using the **PCAP** icon, you can view the PCAP data or download the **PCAP** file to your desktop system.

- 1 Click the **Log Activity** tab.
- 2 From the **Search** list box, select **New Search**.
- 3 Optional. To search for events that have PCAP data, configure the following search criteria:
 - a From the first list box, select **PCAP data**.
 - b From the second list box, select **Equals**.
 - c From the third list box, select **True**.
 - d Click **Add Filter**.
- 4 Configure your column definitions to include the **PCAP Data** column:
 - a From the **Available Columns** list in the Column Definition pane, click **PCAP Data**.
 - b Click the **Add Column** icon on the bottom set of icons to move the **PCAP Data** column to the **Columns** list.
 - c Optional. Click the **Add Column** icon in the top set of icons to move the **PCAP Data** column to the **Group By** list.
- 5 Click **Filter**.
- 6 Optional. If you are viewing events in streaming mode, click the **Pause** icon to pause streaming.
- 7 Double-click the event that you want to investigate.

For more information about viewing and downloading PCAP data, see the following sections:

- [Viewing PCAP information](#)
- [Downloading the PCAP file to your desktop system](#)

Viewing PCAP information

From the **PCAP Data** toolbar menu, you can view a readable version of the data in the PCAP file or download the PCAP file to your desktop system.

Before you can view PCAP information, you must perform or select a search that displays the **PCAP Data** column.

Before PCAP data can be displayed, the PCAP file must be retrieved for display on the user interface. If the download process takes an extended period, the **Downloading PCAP Packet information** window is displayed. In most cases, the download process is quick and this window is not displayed.

After the file is retrieved, a pop-up window provides a readable version of the PCAP file. You can read the information that is displayed on the window, or download the information to your desktop system

- 1 For the event you want to investigate, choose one of the following options:
 - Select the event and click the **PCAP** icon.
 - Right-click the **PCAP** icon for the event and select **More Options > View PCAP Information**.
 - Double-click the event that you want to investigate, and then select **PCAP Data > View PCAP Information** from the event details toolbar.
- 2 If you want to download the information to your desktop system, choose one of the following options:
 - Click **Download PCAP File** to download the original PCAP file to be used in an external application.
 - Click **Download PCAP Text** to download the PCAP information in .TXT format
- 3 Choose one of the following options:
 - If you want to open the file for immediate viewing, select the **Open with** option and select an application from the list box.
 - If you want to save the list, select the **Save File** option.
- 4 Click **OK**.

Downloading the PCAP file to your desktop system

You can download the PCAP file to your desktop system for storage or for use in other applications.

Before you can view a PCAP information, you must perform or select a search that displays the PCAP Data column. See **Displaying the PCAP data column**.

- 1 For the event you want to investigate, choose one of the following options:
 - Select the event and click the **PCAP** icon.
 - Right-click the PCAP icon for the event and select **More Options > Download PCAP File** .
 - Double-click the event you want to investigate, and then select **PCAP Data > Download PCAP File** from the event details toolbar.
- 2 Choose one of the following options:
 - If you want to open the file for immediate viewing, select the **Open with** option and select an application from the list box.
 - If you want to save the list, select the **Save File** option.
- 3 Click **OK**.

Exporting events

You can export events in Extensible Markup Language (XML) or Comma-Separated Values (CSV) format.

The length of time that is required to export your data depends on the number of parameters specified.

- 1 Click the **Log Activity** tab.
- 2 Optional. If you are viewing events in streaming mode, click the **Pause** icon to pause streaming.
- 3 From the **Actions** list box, select one of the following options:
 - **Export to XML > Visible Columns** - Select this option to export only the columns that are visible on the Log Activity tab. This is the recommended option.
 - **Export to XML > Full Export (All Columns)** - Select this option to export all event parameters. A full export can take an extended period of time to complete.
 - **Export to CSV > Visible Columns** - Select this option to export only the columns that are visible on the **Log Activity** tab. This is the recommended option.
 - **Export to CSV > Full Export (All Columns)** - Select this option to export all event parameters. A full export can take an extended period of time to complete.
- 4 If you want to resume your activities while the export is in progress, click **Notify When Done**.

When the export is complete, you receive notification that the export is complete. If you did not select the **Notify When Done** icon, the status window is displayed.

5 Asset Management overview

Asset data sources

Updates to asset data

Asset growth deviations

Example: Asset exclusion rules that are tuned to exclude IP addresses from the blacklist

Example: How configuration errors for log source extensions can cause asset growth deviations

Collecting and viewing asset data helps you to identify threats and vulnerabilities. An accurate asset database makes it easier to connect offenses that are triggered in your system to physical or virtual assets in your network.

Asset data

An *asset* is any network endpoint that sends or receives data across your network infrastructure. For example, notebooks, servers, virtual machines, and handheld devices are all assets. Every asset in the asset database is assigned a unique identifier so that it can be distinguished from other asset records.

Detecting devices is also useful in building a data set of historical information about the asset. Tracking asset information as it changes helps you monitor asset usage across your network.

Asset profiles

An *asset profile* is a collection of all information that Extreme SIEM collected over time about a specific asset. The profile includes information about the services that are running on the asset and any identity information that is known.

Extreme SIEM automatically creates asset profiles from identity events or, if they are configured, vulnerability assessment scans. The data is correlated through a process that is called *asset reconciliation* and the profile is updated as new information comes into Extreme Security. The asset name is derived from the information in the asset update in the following order of precedence:

- Given name
- NETBios host name
- DNS host name
- IP address

Correlating asset profiles to reduce false positives

Administrators use asset profiles to report on, search, audit, and create rules to identify threats, vulnerabilities, and asset usage. The asset data is also used for correlation purposes to help reduce false positives. For example, if an attacker attempts to use a specific service that is running on an asset, Extreme Security can determine whether the asset is vulnerable to this attack by correlating the attack to the asset profile.

Asset data sources

Asset data is received from several different sources in your Extreme Networks Security Analytics deployment.

Asset data is written to the asset database incrementally, usually two or three pieces of data at a time. With exception of updates from network vulnerability scanners, each asset update contains information about only one asset at a time.

Asset data usually comes from one of the following asset data sources:

Events	Event payloads, such as those created by DHCP or authentication servers, often contain user logins, IP addresses, host names, MAC addresses, and other asset information. This data is immediately provided to the asset database to help determine which asset the asset update applies to.
	Events are the primary cause for asset growth deviations.
Vulnerability scanners	Extreme Security integrates with both IBM and third-party vulnerability scanners that can provide asset data such as operating system, installed software, and patch information. The type of data varies from scanner to scanner, and can vary from scan to scan. As new assets, port information, and vulnerabilities are discovered, data is brought into the asset profile based on the CIDR ranges that are defined in the scan.
	It is possible for scanners to introduce asset growth deviations, but it is rare.
User interface	Users who have the Assets role can import or provide asset information directly to the asset database. Asset updates that are provided directly by a user are for a specific asset, and therefore the asset reconciliation stage is bypassed.
	Asset updates that are provided by users do not introduce asset growth deviations.

Domain-aware asset data

When an asset data source is configured with domain information, all asset data that comes from that data source is automatically tagged with the same domain. Because the data in the asset model is domain-aware, the domain information is applied to all Extreme Security components, including identities, offenses, asset profiles, and server discovery.

When you view the asset profile, some fields might be blank. Blank fields exist when the system did not receive this information in an asset update, or the information exceeded the asset retention period. The default retention period is 120 days. An IP address that appears as 0.0.0.0 indicates that the asset does not contain IP address information.

Updates to asset data

Extreme Networks Security Analytics uses identity information in an event payload to determine whether to create a new asset or update an existing asset.

Each asset update must contain trusted information about a single asset. When Extreme Security receives an asset update, the system determines which asset the update applies to.

Asset reconciliation is the process of determining the relationship between asset updates and the related asset in the asset database. Asset reconciliation occurs after Extreme Security receives the update but before the information is written to the asset database.

Identity information

Every asset must contain at least one piece of identity data. Subsequent updates that contain one or more pieces of that same identity data are reconciled with the asset that owns that data. Updates that are based on IP addresses are handled carefully to avoid false-positive asset matches. False-positive asset matches occur when one physical asset is assigned ownership of an IP address that was previously owned by another asset in the system.

When multiple pieces of identity data are provided, the asset profiler prioritizes the information in the following order:

- MAC address (most deterministic)
- NetBIOS host name
- DNS host name
- IP address (least deterministic)

MAC addresses, NetBIOS host names, and DNS host names must be unique and therefore are considered as definitive identity data. Incoming updates that match an existing asset only by the IP address are handled differently than updates that match more definitive identity data.

Asset updates workflow

This workflow describes how Extreme Security uses identity information in an event payload to determine whether to create a new asset or update an existing asset.

- 1 Extreme Security receives the event. The asset profiler examines the event payload for identity information.
- 2 If the identity information includes a MAC address, NetBIOS host names, or DNS host name that are already associated with an asset in the asset database, that asset is updated with any new information.
- 3 If the only available identity information is an IP address, the system reconciles the update to the existing asset that has the same IP address.
- 4 If an asset update includes an IP address that matches an existing asset, but also includes more identity information that does not match the existing asset, the system uses other information to rule out a false-positive match before the existing asset is updated.
- 5 If the identity information does not match an existing asset in the database, a new asset is created based on the information in the event payload.

Related Links

[Asset reconciliation exclusion rules](#) on page 50

With each asset update that enters Extreme Networks Security Analytics, the asset reconciliation exclusion rules apply tests to the MAC address, NetBIOS host name, DNS host name, and IP address in the asset update.

Asset merging

Asset merging is the process where the information for one asset is combined with the information for another asset under the premise that they are actually the same physical asset.

Asset merging occurs when an asset update contains identity data that matches two different asset profiles. For example, a single update that contains a NetBIOS host name that matches one asset profile and a MAC address that matches a different asset profile might trigger an asset merge.

Some systems can cause high volumes of asset merging because they have asset data sources that inadvertently combine identity information from two different physical assets into a single asset update. Some examples of these systems include the following environments:

- Central syslog servers that act as an event proxy
- Virtual machines
- Automated installation environments
- Non-unique host names, common with assets like iPads and iPhones.
- Virtual private networks that have shared MAC addresses
- Log source extensions where the identity field is `OverrideAndAlwaysSend=true`

Assets that have many IP addresses, MAC addresses, or host names show deviations in asset growth and can trigger system notifications.

Related Links

[Asset growth deviations](#) on page 46

Asset growth deviations

Sometimes asset data sources produce updates that cause asset growth deviations in Extreme Networks Security Analytics. *Asset growth deviations* occur when the number of asset updates for an asset outpaces the retention threshold for a specific type of identity information. To maintain the health of the Extreme Security asset database, manual intervention is required to resolve the accumulation of asset data.

Asset profiles are expected to grow and become rich in data over time. For example, the asset profile includes more IP addresses as it collects IP leases, and it collects more user names as new users log in. Asset growth deviations indicate that something is causing the asset profile to collect a large amount of data at an unexpected pace.

DHCP server example of unnatural asset growth in an asset profile

Consider a virtual private network (VPN) server in a Dynamic Host Configuration Protocol (DHCP) network. The VPN server is configured to assign IP addresses to incoming VPN clients by proxying DHCP requests on behalf of the client to the network's DHCP server.

From the perspective of the DHCP server, the same MAC address repeatedly requests many IP address assignments. In the context of network operations, the VPN server is delegating the IP addresses to the clients, but the DHCP server can't distinguish when a request is made by one asset on behalf of another.

The DHCP server log, which is configured as a Extreme Security log source, generates a DHCP acknowledgment (DHCP ACK) event that associates the MAC address of the VPN server with the IP address that it assigned to the VPN client. When asset reconciliation occurs, the system reconciles this event by MAC address, which results in a single existing asset that grows by one IP address for every DHCP ACK event that is parsed.

Eventually, one asset profile contains every IP address that was allocated to the VPN server. This asset growth deviation is caused by asset updates that contain information about more than one asset.

Threshold settings

When an asset in the database reaches a specific number of properties, such as multiple IP addresses or MAC addresses, Extreme Security blocks that asset from receiving more updates.

The Asset Profiler threshold settings specify the conditions under which an asset is blocked from updates. The asset is updated normally up to the threshold value. When the system collects enough data to exceed the threshold, the asset shows an asset growth deviation. Future updates to the asset are blocked until the growth deviation is rectified.

System notifications for asset growth deviations

Extreme Networks Security Analytics generates system notifications to help you identify and manage the asset growth deviations in your environment.

Asset growth deviations, which are unnatural growth of asset data, are specific to an environment.

When an asset is identified as showing a growth deviation, a system notification appears in the **Messages** list on the upper right of the Extreme Security Console. The notifications also appear in the **System Notifications** on the **Systems Monitoring** dashboard.

The following system messages indicate that Extreme Security identified potential asset growth deviations:

- The system detected asset profiles that exceed the normal size threshold
- The asset blacklist rules have added new asset data to the asset blacklists

The system notification messages include links to reports to help you identify the assets that have growth deviations.

Related Links

[Troubleshooting asset profiles that exceed the normal size threshold](#) on page 48

Extreme Networks Security Analytics generates the following system notification when the accumulation of data under a single asset exceeds the configured threshold limits for identity data.

[New asset data is added to the asset blacklists](#) on page 49

Extreme Networks Security Analytics generates the following system notification when a piece of asset data exhibits behavior that is consistent with deviating asset growth.

Troubleshooting asset profiles that exceed the normal size threshold

Extreme Networks Security Analytics generates the following system notification when the accumulation of data under a single asset exceeds the configured threshold limits for identity data.

The system detected asset profiles that exceed the normal size threshold

Explanation

The payload of the notification shows a list of the top five most frequently deviating assets and why the system marked each asset as a growth deviation. As shown in the following example, the payload also shows the number of times that the asset attempted to grow beyond the asset size threshold.

```
Feb 13 20:13:23 127.0.0.1 [AssetProfilerLogTimer]
com.q1labs.assetprofile.updateresolution.UpdateResolutionManager:
[INFO] [NOT:0010006101][9.21.118.83/- -] [-/- -]
The top five most frequently deviating asset profiles between
Feb 13, 2015 8:10:23 PM AST and Feb 13, 2015 8:13:23 PM AST:
[ASSET ID:1003, REASON:Too Many IPs, COUNT:508],
[ASSET ID:1002, REASON:Too many DNS Names, COUNT:93],
[ASSET ID:1001, REASON:Too many MAC Addresses, COUNT:62]
```

When the asset data exceeds the configured threshold, Extreme Security blocks the asset from future updates. This intervention prevents the system from receiving more corrupted data and mitigates the performance impacts that might occur if the system attempts to reconcile incoming updates against an abnormally large asset profile.

Required user action

Use the information in the notification payload to identify the assets that are contributing to the asset growth deviation and determine what is causing the abnormal growth. The notification provides a link to a report of all assets that experienced deviating asset growth over the past 24 hours.

After you resolve the asset growth deviation in your environment, you can run the report again.

- 1 Click the **Log Activity** tab and click **Search > New Search**.
- 2 Select the **Deviating Asset Growth: Asset Report** saved search.
- 3 Use the report to identify and repair inaccurate asset data that was created during the deviation.

If the asset data is valid, Extreme Security administrators can increase the threshold limits for IP addresses, MAC addresses, NetBIOS host names, and DNS host names in the **Asset Profiler Configuration** on the Extreme Security **Admin** tab.

Related Links

[System notifications for asset growth deviations](#) on page 47

Extreme Networks Security Analytics generates system notifications to help you identify and manage the asset growth deviations in your environment.

New asset data is added to the asset blacklists

Extreme Networks Security Analytics generates the following system notification when a piece of asset data exhibits behavior that is consistent with deviating asset growth.

The asset blacklist rules have added new asset data to the asset blacklists

Explanation

Asset exclusion rules monitor asset data for consistency and integrity. The rules track specific pieces of asset data over time to ensure that they are consistently being observed with the same subset of data within a reasonable time.

For example, if an asset update includes both a MAC address and a DNS host name, the MAC address is associated with that DNS host name for a sustained period. Subsequent asset updates that contain that MAC address also contain that same DNS host name when one is included in the asset update. If the MAC address suddenly is associated with a different DNS host name for a short period, the change is monitored. If the MAC address changes again within a short period, the MAC address is flagged as contributing to an instance of deviating or abnormal asset growth.

Required user action

Use the information in the notification payload to identify the rules that are used to monitor asset data. Click the **Asset deviations by log source** link in the notification to see the asset deviations that occurred in the last 24 hours.

If the asset data is valid, Extreme Security administrators can configure Extreme Security to resolve the problem.

- If your blacklists are populating too aggressively, you can tune the asset reconciliation exclusion rules that populate them.
- If you want to add the data to the asset database, you can remove the asset data from the blacklist and add it to the corresponding asset whitelist. Adding asset data to the whitelist prevents it from inadvertently reappearing on the blacklist.

Related Links

[Asset reconciliation exclusion rules](#) on page 50

With each asset update that enters Extreme Networks Security Analytics, the asset reconciliation exclusion rules apply tests to the MAC address, NetBIOS host name, DNS host name, and IP address in the asset update.

[Asset blacklists](#) on page 49

An *asset blacklist* is a collection of data that Extreme Networks Security Analytics considers untrustworthy based on the asset reconciliation exclusion rules. Data in the asset blacklist is likely to contribute to asset growth deviations and Extreme Security prevents the data from being added to the asset database.

Asset blacklists

An *asset blacklist* is a collection of data that Extreme Networks Security Analytics considers untrustworthy based on the asset reconciliation exclusion rules. Data in the asset blacklist is likely to

contribute to asset growth deviations and Extreme Security prevents the data from being added to the asset database.

Every asset update in Extreme Security is compared to the asset blacklists. Blacklisted asset data is applied globally for all domains. If the asset update contains identity information (MAC address, NetBIOS host name, DNS host name, or IP address) that is found on a blacklist, the incoming update is discarded and the asset database is not updated.

The following table shows the reference collection name and type for each type of identity asset data.

Table 17: Reference collection names for asset blacklist data

Type of identity data	Reference collection name	Reference collection type
IP addresses (v4)	Asset Reconciliation IPv4 Blacklist	Reference Set [Set Type: IP]
DNS host names	Asset Reconciliation DNS Blacklist	Reference Set [Set Type: ALNIC*]
NetBIOS host names	Asset Reconciliation NetBIOS Blacklist	Reference Set [Set Type: ALNIC*]
MAC Addresses	Asset Reconciliation MAC Blacklist	Reference Set [Set Type: ALNIC*]

* ALNIC is an alphanumeric type that can accommodate both host name and MAC address values.

Asset reconciliation exclusion rules

With each asset update that enters Extreme Networks Security Analytics, the asset reconciliation exclusion rules apply tests to the MAC address, NetBIOS host name, DNS host name, and IP address in the asset update.

By default, each piece of asset data is tracked over a two-hour period. If any one piece of identity data in the asset update exhibits suspicious behavior two or more times within 2 hours, that piece of data is added to the asset blacklists. There is a separate blacklist for each type of identity asset data that is tested.

In domain-aware environments, the asset reconciliation exclusion rules track the behavior of asset data separately for each domain.

The asset reconciliation exclusion rules test the following scenarios:

Table 18: Rule tests and responses

Scenario	Rule response
When a MAC address is associated to three or more different IP addresses in 2 hours or less	Add the MAC address to the Asset Reconciliation Domain MAC blacklist
When a DNS host name is associated to three or more different IP addresses in 2 hours or less	Add the DNS host name to the Asset Reconciliation Domain DNS blacklist
When a NetBIOS host name is associated to three or more different IP addresses in 2 hours or less	Add the NetBIOS host name to the Asset Reconciliation Domain NetBIOS blacklist
When an IPv4 address is associated to three or more different MAC addresses in 2 hours or less	Add the IP address to the Asset Reconciliation Domain IPv4 blacklist

Table 18: Rule tests and responses (continued)

Scenario	Rule response
When a NetBIOS host name is associated to three or more different MAC addresses in 2 hours or less	Add the NetBIOS host name to the Asset Reconciliation Domain NetBIOS blacklist
When a DNS host name is associated to three or more different MAC addresses in 2 hours or less	Add the DNS host name to the Asset Reconciliation Domain DNS blacklist
When an IPv4 address is associated to three or more different DNS host names in 2 hours or less	Add the IP address to the Asset Reconciliation Domain IPv4 blacklist
When a NetBIOS host name is associated to three or more different DNS host names in 2 hours or less	Add the NetBIOS host name to the Asset Reconciliation Domain NetBIOS blacklist
When a MAC address is associated to three or more different DNS host names in 2 hours or less	Add the MAC address to the Asset Reconciliation Domain MAC blacklist
When an IPv4 address is associated to three or more different NetBIOS host names in 2 hours or less	Add the IP address to the Asset Reconciliation Domain IPv4 blacklist
When a DNS host name is associated to three or more different NetBIOS host names in 2 hours or less	Add the DNS host name to the Asset Reconciliation Domain DNS blacklist
When a MAC address is associated to three or more different NetBIOS host names in 2 hours or less	Add the MAC address to the Asset Reconciliation Domain MAC blacklist

You can view these rules on the **Offenses** tab by clicking **Rules** and then selecting the **asset reconciliation exclusion** group in the drop-down list.

Related Links

[Example: Asset exclusion rules that are tuned to exclude IP addresses from the blacklist](#) on page 51
You can exclude IP addresses from being blacklisted by tuning the asset exclusion rules.

Example: Asset exclusion rules that are tuned to exclude IP addresses from the blacklist

You can exclude IP addresses from being blacklisted by tuning the asset exclusion rules.

As the Network security administrator, you manage a corporate network that includes a public wifi network segment where IP address leases are typically short and frequent. The assets on this segment of the network tend to be transient, primarily notebooks and hand-held devices that log in and out of the public wifi frequently. Commonly, a single IP address is used multiple times by different devices over a short time.

In the rest of your deployment, you have a carefully managed network that consists only of inventoried, well-named company devices. IP address leases are much longer in this part of the network, and IP addresses are accessed by authentication only. On this network segment, you want to know immediately when there are any asset growth deviations and you want to keep the default settings for the asset reconciliation exclusion rules.

Blacklisting IP addresses

In this environment, the default asset reconciliation exclusion rules inadvertently blacklist the entire network in a short time.

Your security team finds the asset-related notifications that are generated by the wifi segment are a nuisance. You want to prevent the wifi from triggering any more deviating asset growth notifications.

Tuning asset reconciliation rules to ignore some asset updates

You review the **Asset deviation by log source** report in the last system notification. You determine that the blacklisted data is coming from the DHCP server on your wifi.

The values in the **Event/Flow Count** column and the **Offenses** column for the row corresponding to the **AssetExclusion: Exclude IP By MAC Address** rule indicate that your wifi DHCP server is triggering this rule.

You add a test to the existing asset reconciliation exclusion rules to stop rules from adding wifi data to the blacklist.

```
Apply AssetExclusion:Exclude IP by MAC address on events which are detected
by
the Local system and NOT when the event(s) were detected by one or more of
MicrosoftDHCP @ microsoft.dhcp.test.com
and NOT when any of Domain is the key and any of Identity IP is the value in
any of Asset Reconciliation Domain IPv4 Whitelist
- IP Asset Reconciliation Domain IPv4 Blacklist - IP
and when at least 3 events are seen with the same Identity IP and
different Identity MAC in 2 hours.
```

The updated rule tests only the events from the log sources that are not on your wifi DHCP server. To prevent wifi DHCP events from undergoing more expensive reference set and behavior analysis tests, you also moved this test to the top of the test stack

Example: How configuration errors for log source extensions can cause asset growth deviations

Customized log source extensions that are improperly configured can cause asset growth deviations.

You configure a customized log source extension to provide asset updates to Extreme Security by parsing user names from the event payload that is on a central log server. You configure the log source extension to override the event host name property so that the asset updates that are generated by the custom log source always specify the DNS host name of the central log server.

Instead of Extreme Security receiving an update that has the host name of the asset that the user logged in to, the log source generates many asset updates that all have the same host name.

In this situation, the asset growth deviation is caused by one asset profile that contains many IP addresses and user names.

6 Chart management

Time series chart overview

Chart legends

Configuring charts

You can use various chart configuration options to view your data.

If you select a time frame or a grouping option to view your data, then the charts display above the event list.

Charts do not display while in streaming mode.

You can configure a chart to select what data you want to plot. You can configure charts independently of each other to display your search results from different perspectives.

Chart types include:

- Bar Chart - Displays data in a bar chart. This option is only available for grouped events.
- Pie Chart - Displays data in a pie chart. This option is only available for grouped events.
- Table - Displays data in a table. This option is only available for grouped events.
- Time Series - Displays an interactive line chart that represents the records that are matched by a specified time interval. For information about configuring time series search criteria, see [Time series chart overview](#).

After you configure a chart, your chart configurations are retained when you:

- Change your view by using the **Display** list box.
- Apply a filter.
- Save your search criteria.

Your chart configurations are not retained when you:

- Start a new search.
- Access a quick search.
- View grouped results in a branch window.
- Save your search results.



Note

If you use the Mozilla Firefox web browser and an ad blocker browser extension is installed, charts do not display. To display charts, you must remove the ad blocker browser extension. For more information, see your browser documentation.

Time series chart overview

Time series charts are graphical representations of your activity over time.

Peaks and valleys that are displayed in the charts depict high and low volume activity. Time series charts are useful for short-term and long term trending of data.

Using time series charts, you can access, navigate, and investigate log or network activity from various views and perspectives.



Note

You must have the appropriate role permissions to manage and view time series charts.

To display time series charts, you must create and save a search that includes time series and grouping options. You can save up to 100 time series searches.

Default time series saved searches are accessible from the list of available searches on the event search page.

You can easily identify saved time series searches on the **Quick Searches** menu, because the search name is appended with the time range specified in the search criteria.

If your search parameters match a previously saved search for column definition and grouping options, a time series chart might automatically display for your search results. If a time series chart does not automatically display for your unsaved search criteria, no previously saved search criteria exists to match your search parameters. If this occurs, you must enable time series data capture and save your search criteria.

You can magnify and scan a timeline on a time series chart to investigate activity. The following table provides functions that you can use to view time series charts.

Table 19: Time series charts functions

Function	Description
View data in greater detail	<p>Using the zoom feature, you can investigate smaller time segments of event traffic.</p> <ul style="list-style-type: none"> Move your mouse pointer over the chart, and then use your mouse wheel to magnify the chart (roll the mouse wheel up). Highlight the area of the chart you want to magnify. When you release your mouse button, the chart displays a smaller time segment. Now you can click and drag the chart to scan the chart. <p>When you magnify a time series chart, the chart refreshes to display a smaller time segment.</p>
View a larger time span of data	<p>Using the zoom feature, you can investigate larger time segments or return to the maximum time range. You can expand a time range using one of the following options:</p> <ul style="list-style-type: none"> Click Zoom Reset at the upper left corner of the chart. Move your mouse pointer over the chart, and then use your mouse wheel to expand the view (roll the mouse wheel down).
Scan the chart	<p>When you have magnified a time series chart, you can click and drag the chart to the left or right to scan the timeline.</p>

Chart legends

Each chart provides a legend, which is a visual reference to help you associate the chart objects to the parameters they represent.

Using the legend feature, you can perform the following actions:

- Move your mouse pointer over a legend item or the legend color block to view more information about the parameters it represents.
- Right-click the legend item to further investigate the item.
- Click a pie or bar chart legend item to hide the item in the chart. Click the legend item again to show the hidden item. You can also click the corresponding graph item to hide and show the item.
- Click **Legend**, or the arrow beside it, if you want to remove the legend from your chart display.

Configuring charts

You can use configuration options to change the chart type, the object type you want to chart, and the number of objects that are represented on the chart. For time series charts, you can also select a time range and enable time series data capture.

Charts are not displayed when you view events in Real Time (streaming) mode. To display charts, you must access the **Log Activity** tab, and choose one of the following options:

- Select options from the **View** and **Display** list boxes, and then click **Save Criteria** on the toolbar. See [Saving event and flow search criteria](#).
- On the toolbar, select a saved search from the **Quick Search** list.
- Perform a grouped search, and then click **Save Criteria** on the toolbar.

If you plan to configure a time series chart, ensure that the saved search criteria is grouped and specifies a time range.

Data can be accumulated so that when you perform a time series search, a cache of data is available to display data for the previous time period. After you enable time series data capture for a selected parameter, an asterisk (*) is displayed next to the parameter in the Value to Graph list box.

- 1 Click the **Log Activity** tab.
- 2 In the Charts pane, click the **Configure** icon.

- 3 Configure values the following parameters:

Option	Description
Parameter	Description
Value to Graph	<p>From the list box, select the object type that you want to graph on the Y axis of the chart.</p> <p>Options include all normalized and custom event parameters included in your search parameters.</p>
Display Top	From the list box, select the number of objects you want to view in the chart. The default is 10. Charting any more than 10 items might cause your chart data to be unreadable.
Chart Type	<p>From the list box, select the chart type that you want to view.</p> <p>If your bar, pie, or table chart is based on saved search criteria with a time range of more than 1 hour, you must click Update Details to update the chart and populate the event details</p>
Capture Time Series Data	<p>Select this check box if you want to enable time series data capture. When you select this check box, the chart feature begins accumulating data for time series charts. By default, this option is disabled.</p> <p>This option is only available on Time Series charts.</p>
Time Range	<p>From the list box, select the time range that you want to view.</p> <p>This option is only available on Time Series charts.</p>

- 4 If you selected the **Time Series** chart option and enabled the **Capture Time Series Data** option, click **Save Criteria** on the toolbar.
- 5 To view the list of events if your time range is greater than 1 hour, click **Update Details**.

7 Data searches

Searching for items that match your criteria

Saving search criteria

Scheduled search

Advanced search options

Quick filter search options

Using a subsearch to refine search results

Managing search results

Managing search groups

On the **Log Activity** tab, you can search events by using specific criteria.

You can create a search or load a previously saved set of search criteria. You can select, organize, and group the columns of data to be displayed in search results.

After you perform a search, you can save the search criteria and the search results.

Searching for items that match your criteria

You can search for data that matches your search criteria.

Since the entire database is searched, searches might take an extended time, depending on the size of your database.

You can use the **Quick Filter** search parameter to search for items that match your text string in the event payload.

The following table describes the search options that you can use to search event and flow data:

Table 20: Search options

Options	Description
Group	Select an event search group to view in the Available Saved Searches list.
Type Saved Search or Select from List	Type the name of a saved search or a keyword to filter the Available Saved Searches list.
Available Saved Searches	This list displays all available searches, unless you use Group or Type Saved Search or Select from List options to apply a filter to the list. You can select a saved search on this list to display or edit.
Search	The Search icon is available in multiple panes on the search page. You can click Search when you are finished configuring the search and want to view the results.

Table 20: Search options (continued)



Options	Description
Include in my Quick Searches	Select this check box to include this search in your Quick Search menu.
Include in my Dashboard	<p>Select this check box to include the data from your saved search on the Dashboard tab. For more information about the Dashboard tab, see Dashboard management.</p> <hr/> <div>  <p>Note This parameter is only displayed if the search is grouped.</p> </div> <hr/>
Set as Default	Select this check box to set this search as your default search.
Share with Everyone	Select this check box to share this search with all other users.
Real Time (streaming)	<p>Displays results in streaming mode. For more information about streaming mode, see Viewing streaming events.</p> <hr/> <div>  <p>Note When Real Time (streaming) is enabled, you are unable to group your search results. If you select any grouping option in the Column Definition pane, an error message opens.</p> </div> <hr/>
Last Interval (auto refresh)	<p>Displays the search results in auto-refresh mode.</p> <p>In auto-refresh mode, the Log Activity tab refresh at one-minute interval to display the most recent information.</p>
Recent	Select a predefined time range for your search. After you select this option, you must select a time range option from the list box.
Specific Interval	Select a custom time range for your search. After you select this option, you must select the date and time range from the Start Time and End Time calendars.
Data Accumulation	<p>This pane is only displayed when you load a saved search.</p> <p>Enabling unique counts on accumulated data that is shared with many other saved searches and reports might decrease system performance.</p> <p>When you load a saved search, this pane displays the following options:</p> <ul style="list-style-type: none"> • If no data is accumulating for this saved search, the following information message is displayed: Data is not being accumulated for this search. • If data is accumulating for this saved search, the following options are displayed: <ul style="list-style-type: none"> • columns - When you click or hover your mouse over this link, a list of the columns that are accumulating data opens. • Enable Unique Counts/Disable Unique Counts - This link allows you to enable or disable the search results to display unique event counts instead of average counts over time. After you click the Enable Unique Counts link, a dialog box opens and indicates which saved searches and reports share the accumulated data.
Current Filters	This list displays the filters that are applied to this search. The options to add a filter are located above Current Filters list.
Save results when the search is complete	Select this check box to save and name the search results.
Display	Select this list to specify a predefined column that is set to display in the search results.

Table 20: Search options (continued)

Options	Description
Type Column or Select from List	You can use field to filter the columns that are listed in the Available Columns list. Type the name of the column that you want to locate or type a keyword to display a list of column names. For example, type Device to display a list of columns that include Device in the column name.
Available Columns	This list displays available columns. Columns that are currently in use for this saved search are highlighted and displayed in the Columns list.
Add and remove column icons (top set)	Use the top set of icons to customize the Group By list. <ul style="list-style-type: none"> • Add Column - Select one or more columns from the Available Columns list and click the Add Column icon. • Remove Column - Select one or more columns from the Group By list and click the Remove Column icon.
Add and remove column icons (bottom set)	Use the bottom set of icon to customize the Columns list. <ul style="list-style-type: none"> • Add Column - Select one or more columns from the Available Columns list and click the Add Column icon. • Remove Column - Select one or more columns from the Columns list and click the Remove Column icon.
Group By	This list specifies the columns on which the saved search groups the results. Use the following options to customize the Group By list further: <ul style="list-style-type: none"> • Move Up - Select a column and move it up through the priority list using the Move Up icon. • Move Down - Select a column and move it down through the priority list using the Move Down icon. <p>The priority list specifies in which order the results are grouped. The search results are grouped by the first column in the Group By list and then grouped by the next column on the list.</p>
Columns	Specifies columns that are chosen for the search. You can select more columns from the Available Columns list. You can further customize the Columns list by using the following options: <ul style="list-style-type: none"> • Move Up - Moves the selected column up the priority list. • Move Down - Moves the selected own the priority list. <p>If the column type is numeric or time-based and there is an entry in the Group By list, then the column includes a list box. Use the list box to choose how you want to group the column.</p> <p>If the column type is group, the column includes a list box to choose how many levels you want to include for the group.</p>

Table 20: Search options (continued)

Options	Description
Order By	From the first list box, select the column by which you want to sort the search results. Then, from the second list box, select the order that you want to display for the search results. Options include Descending and Ascending .
Results Limit	<p>You can specify the number of rows a search returns on the Edit Search window. The Results Limit field also appears on the Results window.</p> <ul style="list-style-type: none"> For a saved search, the limit is stored in the saved search and re-applied when loading the search. When sorting on a column in the search result that has row limit, sorting is done within the limited rows shown in the data grid. For a grouped by search with time series chart turned on, the row limit only applies to the data grid. The Top N dropdown in the time series chart still controls how many time series are drawn in the chart.

- 1 Click the **Log Activity** tab.
- 2 From the **Search** list box, select **New Search**.
- 3 To select a previously saved search:
 - a Choose one of the following options: **From the Available Saved Searches list, select the saved search you want to load. In the Type Saved Search or Select from List field, type the name of the search you want to load.**
 - b Click **Load**.
 - c In the Edit Search pane, select the options that you want for this search. See Table 1.
- 4 To create a search, in the Time Range pane, select the options for the time range you want to capture for this search.
- 5 Optional. In the Data Accumulation pane, enable unique counts:
 - a Click **Enable Unique Counts**.
 - b On the **Warning** window, read the warning message and click **Continue**. For more information about enabling unique counts, see Table 1.
- 6 In the Search Parameters pane, define your search criteria:
 - a From the first list box, select a parameter that you want to search for. For example, Device, Source Port, or Event Name.
 - b From the second list box, select the modifier that you want to use for the search.
 - c In the entry field, type specific information that is related to your search parameter.
 - d Click **Add Filter**.
 - e Repeat steps a through d for each filter you want to add to the search criteria.
- 7 Optional. To automatically save the search results when the search is complete, select the **Save results when search is complete** check box, and then type a name for the saved search.
- 8 In the Column Definition pane, define the columns and column layout you want to use to view the results:
 - a From the **Display** list box, select the preconfigured column that is set to associate with this search.
 - b Click the arrow next to **Advanced View Definition** to display advanced search parameters.
 - c Customize the columns to display in the search results. See Table 1.
 - d Optional. In the **Results Limit** field, type the number of rows that you want the search to return .

- 9 Click **Filter**.

The **In Progress (<percent>%Complete)** status is displayed in the upper right corner.

.

While viewing partial search results, the search engine works in the background to complete the search and refreshes the partial results to update your view.

When the search is complete, the **Completed** status is displayed in the upper right corner.

Related Links

[Advanced search options](#) on page 63

Use the **Advanced Search** field to enter an Ariel Query Language (AQL) that specifies the fields that you want and how you want to group them to run a query.

[AQL search string examples](#) on page 65

Use the Ariel Query Language (AQL) to retrieve specific fields from the events, flows, and simarc tables in the Ariel database.

Saving search criteria


You can save configured search criteria so that you can reuse the criteria and use the saved search criteria in other components, such as reports. Saved search criteria does not expire.

If you specify a time range for your search, then your search name is appended with the specified time range. For example, a saved search named Exploits by Source with a time range of Last 5 minutes becomes Exploits by Source - Last 5 minutes.

If you change a column set in a previously saved search, and then save the search criteria using the same name, previous accumulations for time series charts are lost.

- 1 Click the **Log Activity** tab.
- 2 Perform a search.
- 3 Click **Save Criteria**.

- 4 Enter values for the parameters:

Option	Description
Parameter	Description
Search Name	Type the unique name that you want to assign to this search criteria.
Assign Search to Group(s)	Select the check box for the group you want to assign this saved search. If you do not select a group, this saved search is assigned to the Other group by default. For more information, see Managing search groups .
Manage Groups	Click Manage Groups to manage search groups. For more information, see Managing search groups .
Timespan options:	Choose one of the following options: <ul style="list-style-type: none"> • Real Time (streaming) - Select this option to filter your search results while in streaming mode. • Last Interval (auto refresh) - Select this option to filter your search results while in auto-refresh mode. The Log Activity and Network Activity tabs refreshes at one-minute intervals to display the most recent information. • Recent - Select this option and, from this list box, select the time range that you want to filter for. • Specific Interval - Select this option and, from the calendar, select the date and time range you want to filter for.
Include in my Quick Searches	Select this check box to include this search in your Quick Search list box on the toolbar.
Include in my Dashboard	Select this check box to include the data from your saved search on the Dashboard tab. For more information about the Dashboard tab, see Dashboard management .
<div>  <div> Note This parameter is only displayed if the search is grouped. </div> </div>	
Set as Default	
Share with Everyone	Select this check box to share these search requirements with all users.

- 5 Click OK.

Scheduled search

Use the Scheduled search option to schedule a search and view the results.

You can schedule a search that runs at a specific time of day or night.

Example

If you schedule a search to run in the night, you can investigate in the morning. Unlike reports, you have the option of grouping the search results and investigating further. You can search on number of failed logins in your network group. If the result is typically 10 and the result of the search is 100, you can group the search results for easier investigating. To see which user has the most failed logins, you can group by user name. You can continue to investigate further.

You can schedule a search on events or flows from the **Reports** tab. You must select a previously saved set of search criteria for scheduling.

1 Create a report

Specify the following information in the **Report Wizard** window:

- The chart type is Events/Logs or Flows.
- The report is based on a saved search.
- Generate an offense.

You can choose the **create an individual offense** option or the **add result to an existing offense** option.

You can also generate a manual search.

2 View search results

You can view the results of your scheduled search from the **Offenses** tab.

- Scheduled search offenses are identified by the **Offense Type** column.

If you create an individual offense, an offense is generated each time that the report is run. If you add the saved search result to an existing offense, an offense is created the first time that the report runs. Subsequent report runs append to this offense. If no results are returned, the system does not append or create an offense.

- To view the most recent search result in the **Offense Summary** window, double-click a scheduled search offense in the offense list. To view the list of all scheduled search runs, click **Search Results** in the **Last 5 Search Results** pane.

You can assign a Scheduled search offense to a user.

Related Links

[Advanced search options](#) on page 63

Use the **Advanced Search** field to enter an Ariel Query Language (AQL) that specifies the fields that you want and how you want to group them to run a query.

[AQL search string examples](#) on page 65

Use the Ariel Query Language (AQL) to retrieve specific fields from the events, flows, and simarc tables in the Ariel database.

Advanced search options

Use the **Advanced Search** field to enter an Ariel Query Language (AQL) that specifies the fields that you want and how you want to group them to run a query.

The **Advanced Search** field has auto completion and syntax highlighting.

Use auto completion and syntax highlighting to help create queries. For information about supported web browsers, see [Supported web browsers](#) on page 11

Accessing Advanced Search

Access the **Advanced Search** option from the **Search** toolbar that is on the **Log Activity** tab to type an AQL query.

Select **Advanced Search** from the list box on the **Search** toolbar.

Expand the **Advanced Search** field by following these steps:

- 1 Drag the expand icon that is at the right of the field.
- 2 Press Shift + Enter to go to the next line.
- 3 Press Enter.

You can right-click any value in the search result and filter on that value.

Double-click any row in the search result to see more detail.

All searches, including AQL searches, are included in the audit log.

AQL search string examples

The following table provides examples of AQL search strings.

Table 21: Examples of AQL search strings

Description	Example
Select default columns from events.	<code>SELECT * FROM events</code>
Select specific columns.	<code>SELECT sourceip, destinationip FROM events</code>
Select specific columns and order the results.	<code>SELECT sourceip, destinationip FROM events ORDER BY destinationip</code>
Run an aggregated search query.	<code>SELECT sourceip, SUM(magnitude) AS magsum FROM events GROUP BY sourceip</code>
Run a function call in a SELECT clause.	<code>SELECT CATEGORYNAME(category) AS namedCategory FROM events</code>
Filter the search results by using a WHERE clause.	<code>SELECT CATEGORYNAME(category) AS namedCategory, magnitude FROM events WHERE magnitude > 1</code>
Search for events that triggered a specific rule, which is based on the rule name or partial text in the rule name.	<code>SELECT LOGSOURCENAME(logsourceid), * from events where RULENAME(creeventlist) ILIKE '%suspicious%'</code>
Reference field names that contain special characters, such as arithmetic characters or spaces, by enclosing the field name in double quotation marks.	<code>SELECT sourceip, destinationip, "+field/name+" FROM events WHERE "+field/name+" LIKE '%test%'</code>

For more information about functions, search fields and operators, see the *Ariel Query Language guide*.

Related Links

[Scheduled search](#) on page 62

Use the Scheduled search option to schedule a search and view the results.

[Searching for items that match your criteria](#) on page 57

You can search for data that matches your search criteria.

[Quick filter search options](#) on page 68

Search event and flow payloads by typing a text search string that uses simple words or phrases.

AQL search string examples

Use the Ariel Query Language (AQL) to retrieve specific fields from the events, flows, and simarc tables in the Ariel database.

Reporting account usage

Different user communities can have different threat and usage indicators.

Use reference data to report on several user properties, for example, department, location, or manager.

You can use external reference data.

The following query returns metadata information about the user from their login events.

```
SELECT
  REFERENCE('user_data','FullName',username) as 'Full Name',
  REFERENCE('user_data','Location',username) as 'Location',
  REFERENCE('user_data','Manager',username) as 'Manager',
  UNIQUECOUNT(username) as 'Userid Count',
  UNIQUECOUNT(sourceip) as 'Source IP Count',
  COUNT(*) as 'Event Count'
FROM events
WHERE qidname(qid) ILIKE '%logon%'
GROUP BY 'Full Name', 'Location', 'Manager'
LAST 1 days
```

Insight across multiple account identifiers

In this example, individual users have multiple accounts across the network. The organization requires a single view of a users activity.

Use reference data to map local user IDs to a global ID.

The following query returns the user accounts that are used by a global ID on events that are flagged as suspicious.

```
SELECT
  REFERENCEMAP('GlobalID Mapping',username) as 'Global ID',
  REFERENCE('user_data','FullName', 'Global ID') as 'Full Name',
  UNIQUECOUNT(username),
  COUNT(*) as 'Event count'
FROM events
WHERE RULENAME(creEventlist) ILIKE '%suspicious%'
GROUP BY 'Global ID'
LAST 1 days
```

The following query shows the activities that are completed by a global ID.

```
SELECT
  QIDNAME(qid) as 'Event name',
  starttime as Time,
  sourceip as 'Source IP', destinationip as 'Destination IP',
  username as 'Event Username',
  REFERENCEMAP('GlobalID_Mapping', username) as 'Global User'
FROM events
WHERE 'Global User' = 'John Doe'
LAST 1 days
```

Identify suspicious long-term beaconing

Many threats use command and control to communicate periodically over days, weeks, and months.

Advanced searches can identify connection patterns over time. For example, you can query consistent, short, low volume, number of connections per day/week/month between IP addresses, or an IP address and geographical location.

Use the Extreme Networks Security Analytics REST API to generate an offense or to populate a reference set or reference table.

The following query detects daily beaconing to a domain by using proxy log events. The beaconing times are not at the same time each day. The time lapse between beacons is short.

```
SELECT
  sourceip,
  DATEFORMAT(starttime, 'hh') as hourofday,
  (AVG(hourofday*hourofday) - (AVG(hourofday)^2)) as variance,
  COUNT(*) as 'total events'
FROM events
WHERE LOGSOURCEGROUPNAME(devicegrouplist) ILIKE '%proxy%'
GROUP BY url_domain
HAVING variance < 0.1 and 'total events' < 10
LAST 7 days
```

The `url_domain` property is a custom property from proxy logs.

External threat intelligence

Usage and security data that is correlated with external threat intelligence data can provide important threat indicators.

Advanced searches can cross-reference external threat intelligence indicators with other security events and usage data.

This query shows how you can profile external threat data over many days, weeks, or months to identify and prioritize the risk level of assets and accounts.

```
Select
  REFERENCEMAP('ip_threat_data', 'Category', destinationip) as 'Category',
  REFERENCEMAP('ip_threat_data', 'Rating', destinationip) as 'Threat Rating',
  UNIQUECOUNT(sourceip) as 'Source IP Count',
```

```

UNIQUECOUNT(destinationip) as 'Destination IP Count'
FROM events
GROUP BY 'Category', 'Threat Rating'
LAST 1 days

```

Asset intelligence and configuration

Threat and usage indicators vary by asset type, operating system, vulnerability posture, server type, classification, and other parameters.

In this query, advanced searches and the asset model provide operational insight into a location.

The *Assetproperty* function retrieves property values from assets, which enables you to include asset data in the results.

```

SELECT
ASSETPROPERTY('Location',sourceip) as location,
COUNT(*) as 'event count'
FROM events
GROUP BY location
LAST 1 days

```

Network LOOKUP function

You can use the *Network LOOKUP* function to retrieve the network name that is associated with an IP address.

```

SELECT NETWORKNAME(sourceip) as srcnet,
NETWORKNAME(destinationip) as dstnet
FROM events

```

Rule LOOKUP function

You can use the *Rule LOOKUP* function to retrieve the name of a rule by its ID.

```

SELECT RULENAME(123) FROM events

```

The following query returns events that triggered a specific rule name.

```

SELECT * FROM events
WHERE RULENAME(creEventList) ILIKE '%my rule name%'

```

Full TEXT SEARCH

You can use the TEXT SEARCH operator to do full text searches by using the **Advanced search** option.

In this example, there are a number of events that contain the word "firewall" in the payload. You can search for these events by using the **Quick filter** option and the **Advanced search** option on the **Log Activity** tab.

- To use the **Quick filter** option, type the following text in the **Quick filter** box: 'firewall'

- To use the **Advanced search** option, type the following query in the **Advanced search** box:

```
SELECT QIDNAME(qid) AS EventName, * from events where TEXT SEARCH 'firewall'
```

Custom property

You can access custom properties for events and flows when you use the **Advanced search** option.

The following query uses the custom property "MyWebsiteUrl" to sort events by a particular web URL:

```
SELECT "MyWebsiteUrl", * FROM events ORDER BY "MyWebsiteUrl"
```

Related Links

[Scheduled search](#) on page 62

Use the Scheduled search option to schedule a search and view the results.

[Searching for items that match your criteria](#) on page 57

You can search for data that matches your search criteria.

[Quick filter search options](#) on page 68

Search event and flow payloads by typing a text search string that uses simple words or phrases.

Quick filter search options

Search event and flow payloads by typing a text search string that uses simple words or phrases.

You can filter your searches from these locations:

Log Activity toolbar and toolbars	Select Quick Filter from the list box on the Search toolbar to type a text search string. Click the Quick Filter icon to apply your to the list of events or flows.
Add Filter Dialog box	Click the Add Filter icon on the Log Activity or tab. Select Quick Filter as your filter parameter and type a text search string.
Flow search pages	Add a quick filter to your list of filters.

When you view in real-time (streaming) or last interval mode, you can type only simple words or phrases in the **Quick Filter** field. When you view **events** or in a time-range, follow these syntax guidelines:

Quick filter syntax guidelines

Table 22: Quick filter syntax guidelines

Description	Example
Include any plain text that you expect to find in the payload.	Firewall
Search for exact phrases by including multiple terms in double quotation marks.	"Firewall deny"
Include single and multiple character wildcards. The search term cannot start with a wildcard.	F?rewall or F??ew*
Group terms with logical expressions, such as AND, OR, and NOT. To be recognized as logical expressions and not as search terms, the syntax and operators must be uppercase.	(%PIX* AND ("Accessed URL" OR "Deny udp src") AND 10.100.100.*)

Table 22: Quick filter syntax guidelines (continued)

Description	Example
When you create search criteria that includes the NOT logical expression, you must include at least one other logical expression type, otherwise, no results are returned.	(%PIX* AND ("Accessed URL" OR "Deny udp src") NOT 10.100.100.*)
Precede the following characters by a backslash to indicate that the character is part of your search term: + - && ! () { } [] ^ " ~ * ? : \ .	"%PIX\ -5\ -304001"

Search terms are matched in sequence from the first character in the payload word or phrase. The search term `user` matches `user_1` and `user_2`, but does not match the following phrases: `ruser`, `myuser`, or `anyuser`.

Quick filter searches use the English locale. *Locale* is a setting that identifies language or geography and determines formatting conventions such as collation, case conversion, character classification, the language of messages, date and time representation, and numeric representation.

The locale is set by your operating system. You can configure Extreme Security to override the operating system locale setting. For example, you can set the locale to **English** and the Extreme Security Console can be set to **Italiano (Italian)**.

If you use Unicode characters in your Quick filter search query, unexpected search results might be returned.

If you choose a locale that is not English, you can use the Advanced search option in Extreme Security for searching event and payload data.

Related Links

[Advanced search options](#) on page 63

Use the **Advanced Search** field to enter an Ariel Query Language (AQL) that specifies the fields that you want and how you want to group them to run a query.

[AQL search string examples](#) on page 65

Use the Ariel Query Language (AQL) to retrieve specific fields from the events, flows, and simarc tables in the Ariel database.

Using a subsearch to refine search results

You can use a subsearch to search within a set of completed search results. The subsearch is used to refine search results, without searching the database again.

When you define a search that you want to use as a base for subsearching, make sure that Real Time (streaming) option is disabled and the search is not grouped.

This feature is not available for grouped searches, searches in progress, or in streaming mode.

- 1 Click the **Log Activity** tab.
- 2 Perform a search.

- 3 When your search is complete, add another filter:
 - a Click **Add Filter**.
 - b From the first list box, select a parameter that you want to search for.
 - c From the second list box, select the modifier that you want to use for the search. The list of modifiers that are available depends on the attribute that is selected in the first list.
 - d In the entry field, type specific information that is related to your search.
 - e Click **Add Filter**.

The Original Filter pane specifies the original filters that are applied to the base search. The Current^{*} Filter pane specifies the filters that are applied to the subsearch. You can clear subsearch filters without restarting the base search. Click the **Clear Filter** link next to the filter you want to clear. If you clear a filter from the Original Filter pane, the base search is relaunched.

If you delete the base search criteria for saved subsearch criteria, you still have access to saved subsearch criteria. If you add a filter, the subsearch searches the entire database since the search function no longer bases the search on a previously searched data set.

[Save search criteria](#)

Managing search results

You can initiate multiple searches, and then navigate to other tabs to perform other tasks while your searches complete in the background.

You can configure a search to send you an email notification when the search is complete.

At any time while a search is in progress, you can return to the **Log Activity** tab to view partial or complete search results.

Deleting search criteria

You can delete search criteria.

When you delete a saved search, then objects that are associated with the saved search might not function. Reports and anomaly detection rules are Extreme Security objects that use saved search criteria. After you delete a saved search, edit the associated objects to ensure that they continue to function.

- 1 Click the **Log Activity** tab.
- 2 From the **Search** list box, select **New Search** or **Edit Search**.
- 3 In the Saved Searches pane, select a saved search from the **Available Saved Searches** list box.
- 4 Click **Delete**.
 - If the saved search criteria is not associated with other Extreme Security objects, a confirmation window is displayed.
 - If the saved search criteria is associated with other objects, the **Delete Saved Search** window is displayed. The window lists objects that are associated with the saved search that you want to delete. Note the associated objects.
- 5 Click **OK**.

6 Choose one of the following options:

- Click **OK** to proceed.
- Click **Cancel** to close the **Delete Saved Search** window.

If the saved search criteria was associated with other Extreme Security objects, access the associated objects that you noted and edit the objects to remove or replace the association with the deleted saved search.

Saving search results

You can save the search results.

If you perform a search and do not explicitly save the search results, the search results are available on **Manage Search Windows** for 24 hours and then are automatically deleted.

- 1 Click the **Log Activity** tab.
- 2 Perform a search.
- 3 Click **Save Results**.
- 4 On the **Save Search Result** window, type a unique name for the search results.
- 5 Click **OK**.

Viewing managed search results

Using the **Manage Search Results** page, you can view partial or complete search results.

Saved search results retain chart configurations from the associated search criteria, however, if the search result is based on search criteria that has been deleted, the default charts (bar and pie) are displayed.

The **Manage Search Results** page provides the following parameters

Table 23: Manage search results page parameters

Parameter	Description
Flags	Indicates that an email notification is pending for when the search is complete.
User	Specifies the name of the user who started the search.
Name	Specifies the name of the search, if the search has been saved. For more information about saving a search, see Saving search results .
Started On	Specifies the date and time the search was started.
Ended On	Specifies the date and time the search ended.
Duration	Specifies the amount of time the search took to complete. If the search is in progress, the Duration parameter specifies how long the search has been processing to date. If the search was canceled, the Duration parameter specifies the period of time the search was processing before it was canceled.
Expires On	Specifies the date and time an unsaved search result will expire. The saved search retention figure is configured in the system settings. For more information about configuring system settings, see the <i>Extreme Networks Security Log Manager Administration Guide</i> .

Table 23: Manage search results page parameters (continued)

Parameter	Description
Status	Specifies the status of the search. The statuses are: <ul style="list-style-type: none"> • Queued - Specifies that the search is queued to start. • <percent>%Complete - Specifies the progress of the search in terms of percentage complete. You can click the link to view partial results. • Sorting - Specifies that the search has finished collecting results and is currently preparing the results for viewing. • Canceled - Specifies that the search has been canceled. You can click the link to view the results that were collected before the cancellation. • Completed - Specifies that the search is complete. You can click the link to view the results. See Log activity monitoring
Size	Specifies the file size of the search result set.

The **Manage Search Results** window toolbar provides the following functions

Table 24: Manage Search Results toolbar

Function	Description
New Search	Click New Search to create a new search. When you click this icon, the search page is displayed.
Save Results	Click Save Results to save the selected search results. See Saving search results.
Cancel	Click Cancel to cancel the selected search result that is in progress or are queued to start. See Canceling a search.
Delete	Click Delete to delete the selected search result. See Deleting a search result.
Notify	Click Notify to enable email notification when the selected search is complete.
View	From this list box, you can select which search results you want to list on the Search Results page. The options are: <ul style="list-style-type: none"> • Saved Search Results • All Search Results • Canceled/Erroneous Searches • Searches in Progress

- 1 Click the **Log Activity** tab.
- 2 From the **Search** menu, select **Manage Search Results**.
- 3 View the list of search results.

Canceling a search

While a search is queued or in progress, you can cancel the search on the **Manage Search Results** page.

If the search is in progress when you cancel it, the results that were accumulated until the cancellation are maintained.

- 1 Click the **Log Activity** tab.
- 2 From the **Search** menu, select **Manage Search Results**.
- 3 Select the queued or in progress search result you want to cancel.

- 4 Click **Cancel**.
- 5 Click **Yes**.

Deleting a search

If a search result is no longer required, you can delete the search result from the **Manage Search Results** page.

- 1 Click the **Log Activity** tab.
- 2 From the **Search** menu, select **Manage Search Results**.
- 3 Select the search result that you want to delete.
- 4 Click **Delete**.
- 5 Click **Yes**.

Managing search groups

Using the **Search Groups** window, you can create and manage event, flow, and offense search groups.

These groups allow you to easily locate saved search criteria on the **Log Activity** tab and in the Report wizard.

Viewing search groups

A default set of groups and subgroups are available.

You can view search groups on the **Event Search Group** window.

All saved searches that are not assigned to a group are in the **Other** group.

The **Event Search Group** window displays the following parameters for each group.

Table 25: Search Group window parameters

Parameter	Description
Name	Specifies the name of the search group.
User	Specifies the name of the user that created the search group.
Description	Specifies the description of the search group.
Date Modified	Specifies the date the search group was modified.

The **Event Search Group** window toolbar provides the following functions.

Table 26: Search Group window toolbar functions

Function	Description
New Group	To create a new search group, you can click New Group . See Creating a new search group .
Edit	To edit an existing search group, you can click Edit . See Editing a search group .

Table 26: Search Group window toolbar functions (continued)

Function	Description
Copy	To copy a saved search to another search group, you can click Copy . See Copying a saved search to another group .
Remove	To remove a search group or a saved search from a search group, select the item that you want to remove, and then click Remove . See Removing a group or a saved search from a group .

- 1 Click the **Log Activity** tab.
- 2 **Select Search >Edit Search**.
- 3 Click **Manage Groups**.
- 4 View the search groups.

Creating a new search group

You can create a new search group.

- 1 Click the **Log Activity** tab.
- 2 **Select Search Edit Search**.
- 3 Click **Manage Groups**.
- 4 Select the folder for the group under which you want to create the new group.
- 5 Click **New Group**.
- 6 In the **Name** field, type a unique name for the new group.
- 7 Optional. In the **Description** field, type a description.
- 8 Click **OK**.

Editing a search group

You can edit the **Name** and **Description** fields of a search group.

- 1 Click the **Log Activity** tab.
- 2 Select **Search > Edit Search**.
- 3 Click **Manage Groups**.
- 4 Select the group that you want edit.
- 5 Click **Edit**.
- 6 Edit the parameters:
 - Type a new name in the **Name** field.
 - Type a new description in the **Description** field.
- 7 Click **OK**.

Copying a saved search to another group

You can copy a saved search to one or more groups.

- 1 Click the **Log Activity** tab.

- 2 Select **Search > Edit Search**.
- 3 Click **Manage Groups**.
- 4 Select the saved search that you want to copy.
- 5 Click **Copy**.
- 6 On the **Item Groups** window, select the check box for the group you want to copy the saved search to.
- 7 Click **Assign Groups**.

Removing a group or a saved search from a group

You can use the **Remove** icon to remove a search from a group or remove a search group.

When you remove a saved search from a group, the saved search is not deleted from your system. The saved search is removed from the group and automatically moved to the **Other** group.

You cannot remove Event Search Groups from your system.

- 1 Click the **Log Activity** tab.
- 2 Select **Search > Edit Search**.
- 3 Click **Manage Groups**.
- 4 Choose one of the following options:
 - Select the saved search that you want to remove from the group.
 - Select the group that you want to remove.
- 5 Click **Remove**.
- 6 Click **OK**.

8 Custom event properties

Required permissions

Custom property types

Creating a regex-based custom property

Creating a calculation-based custom property

Modifying a custom property

Copying a custom property

Deleting a custom property

Custom event and flow properties allow you to search, view, and report on information within logs that Extreme SIEM does not typically normalize and display.

You can create custom event properties from several locations on the **Log Activity** tab:

- Event details - You can select an event from the **Log Activity** tab to create a custom event property that is derived from its payload.
- Search page - You can create and edit a custom event or property from the **Search** page. When you create a new custom property from the **Search** page, the property is not derived from any particular event; therefore, the **Custom Property Definition** window does not prepopulate. You can copy and paste payload information from another source.

Required permissions

To create custom properties if you have the correct permission.

You must have the User Defined Event Properties permission.

If you have Administrative permissions, you can also create and modify custom properties from the Admin tab.

Click **Admin > Data Sources > Custom Event Properties**.

Check with your administrator to ensure that you have the correct permissions.

For more information, see the *Extreme Networks Security Log Manager Administration Guide*.

Custom property types

You can create a custom property type.

When you create a custom property, you can choose to create a Regex or a calculated property type.

Using regular expression (Regex) statements, you can extract unnormalized data from event payloads.

For example, a report is created to report all users who make user permission changes on an Oracle server. A list of users and the number of times they made a change to the permission of another account is reported. However, typically the actual user account or permission that was changed cannot display. You can create a custom property to extract this information from the logs, and then use the property in searches and reports. Use of this feature requires advanced knowledge of regular expressions (regex).

Regex defines the field that you want to become the custom property. After you enter a regex statement, you can validate it against the payload. When you define custom regex patterns, adhere to regex rules as defined by the Java™ programming language.

For more information, you can refer to regex tutorials available on the web. A custom property can be associated with multiple regular expressions.

When an event is parsed, each regex pattern is tested on the event until a regex pattern matches the payload. The first regex pattern to match the event payload determines the data to be extracted.

Using calculation-based custom properties, you can perform calculations on existing numeric event or flow properties to produce a calculated property

For example, you can create a property that displays a percentage by dividing one numeric property by another numeric property.

Creating a regex-based custom property

You can create a regex-based custom property to match event or flow payloads to a regular expression.

When you configure a regex-based custom property, the **Custom Event Property** window provides parameters. The following table describes some of these parameters.

Table 27: Custom Event Properties window parameters (regex)

Parameter	Description
Test field	Specifies the payload that was extracted from the unnormalized event or flow. Specifies the payload that was extracted from the unnormalized event.
New Property	The new property name cannot be the name of a normalized property, such as username , Source IP , or Destination IP .
Optimize parsing for rules, reports, and searches	Parses and stores the property the first time that the event or flow is received. When you select the check box, the property does not require more parsing for reporting, searching, or rule testing. If you clear this check box, the property is parsed each time a report, search, or rule test is applied.
Log Source	If multiple log sources are associated with this event, this field specifies the term Multiple and the number of log sources.

Table 27: Custom Event Properties window parameters (regex) (continued)

Parameter	Description
RegEx	<p>The regular expression that you want to use for extracting the data from the payload. Regular expressions are case-sensitive.</p> <p>The following examples show sample regular expressions:</p> <ul style="list-style-type: none"> Email: (.+@[^\ .] . * \ . [a-z] { 2 , } \$) URL: (http \ : / / [a-zA-Z0-9 \ - \ .] + \ . [a-zA-Z] { 2 , 3 } (/ \ S *) ? \$) Domain Name: (http [s] ? : / / (. + ?) [" / ? :]) Floating Point Number: ([- +] ? \ d * \ . ? \ d * \$) Integer: ([- +] ? \ d * \$) IP address: (\ b \ d { 1 , 3 } \ . \ d { 1 , 3 } \ . \ d { 1 , 3 } \ . \ d { 1 , 3 } \ b) <p>Capture groups must be enclosed in parentheses.</p>
Capture Group	Capture groups treat multiple characters as a single unit. In a capture group, characters are grouped inside a set of parentheses.
Enabled	If you clear the check box, this custom property does not display in search filters or column lists and the property is not parsed from payloads.

- 1 Click the **Log Activity** tab.
- 2 If you are viewing events in streaming mode, click the **Pause** icon to pause streaming.
- 3 Double-click the event that you want to base the custom property on
- 4 Click **Extract Property**.
- 5 In the **Property Type Selection** pane, select the **Regex Based** option.
- 6 Configure the custom property parameters.
- 7 Click **Test** to test the regular expression against the payload.
- 8 Click **Save**.

The custom property is displayed as an option in the list of available columns on the search page. To include a custom property in an events or flows list, you must select the custom property from the list of available columns when you create a search.

Creating a calculation-based custom property

You can create a calculation-based custom property to match payloads to a regular expression.

When you configure a calculation-based custom property, the **Custom Event Property** or **Custom Flow Property** windows provide the following parameters:

Table 28: Custom property definition window parameters (calculation)

Parameter	Description
Property Definition	
Property Name	Type a unique name for this custom property. The new property name cannot be the name of a normalized property, such as Username , Source IP , or Destination IP .
Description	Type a description of this custom property.
Property Calculation Definition	

Table 28: Custom property definition window parameters (calculation) (continued)

Parameter	Description
Property 1	From the list box, select the first property that you want to use in your calculation. Options include all numeric normalized and numeric custom properties. You can also specify a specific numeric value. From the Property 1 list box, select the User Defined option. The Numeric Property parameter is displayed. Type a specific numeric value.
Operator	From the list box, select the operator that you want to apply to the selected properties in the calculation. Options include: <ul style="list-style-type: none"> Add Subtract Multiply Divide
Property 2	From the list box, select the second property that you want to use in your calculation. Options include all numeric normalized and numeric custom properties. You can also specify a specific numeric value. From the Property 1 list box, select the User Defined option. The Numeric Property parameter is displayed. Type a specific numeric value.
Enabled	Select this check box to enable this custom property. If you clear the check box, this custom property does not display in event search filters or column lists and the event or flow property is not parsed from payloads.

- 1 Choose one of the following: Click the **Log Activity** tab.
- 2 Optional. If you are viewing events or flows in streaming mode, click the **Pause** icon to pause streaming.
- 3 Double-click the event you want to base the custom property on.
- 4 Click **Extract Property**.
- 5 In the Property Type Selection pane, select the **Calculation Based** option.
- 6 Configure the custom property parameters.
- 7 Click **Test** to test the regular expression against the payload.
- 8 Click **Save**.

The custom property is now displayed as an option in the list of available columns on the search page. To include a custom property in an events or flows list, you must select the custom property from the list of available columns when creating a search.

Modifying a custom property

You can modify a custom property.

You can use the **Custom Event Properties** window to modify a custom property.

The custom properties are described in the following table.

Table 29: Custom properties window columns

Column	Description
Property Name	Specifies a unique name for this custom property.
Type	Specifies the type for this custom property.

Table 29: Custom properties window columns (continued)

Column	Description
Property Description	Specifies a description for this custom property.
Log Source Type	Specifies the name of the log source type to which this custom property applies. This column is only displayed on the Custom Event Properties window.
Log Source	Specifies the log source to which this custom property applies. If there are multiple log sources that are associated with this event, this field specifies the term Multiple and the number of log sources. This column is only displayed on the Custom Event Properties window.
Expression	Specifies the expression for this custom property. The expression depends on the custom property type: For a regex-based custom property, this parameter specifies the regular expression that you want to use for extracting the data from the payload. For a calculation-based custom property, this parameter specifies the calculation that you want to use to create the custom property value.
Username	Specifies the name of the user who created this custom property.
Enabled	Specifies whether this custom property is enabled. This field specifies either True or False.
Creation Date	Specifies the date this custom property was created.
Modification Date	Specifies the last time this custom property was modified.

The Custom Event Property toolbar provides the following functions:

Table 30: Custom property toolbar options

Option	Description
Add	Click Add to add a new custom property.
Edit	Click Edit to edit the selected custom property.
Copy	Click Copy to copy selected custom properties.
Delete	Click Delete to delete selected custom properties.
Enable/Disable	Click Enable/Disable to enable or disable the selected custom properties for parsing and viewing in the search filters or column lists.

- 1 Click the **Log Activity** tab.
- 2 From the **Search** list box, select **Edit Search**.
- 3 Click **Manage Custom Properties**.
- 4 Select the custom property that you want to edit and click **Edit**.
- 5 Edit the necessary parameters.

- 6 Optional. If you edited the regular expression, click **Test** to test the regular expression against the payload.
- 7 Click **Save**.

Copying a custom property

To create a new custom property that is based on an existing custom property, you can copy the existing custom property, and then modify the parameters.

- 1 Click the **Log Activity** tab.
- 2 From the **Search** list box, select **Edit Search**.
- 3 Click **Manage Custom Properties**.
- 4 Select the custom property that you want to copy and click **Copy**.
- 5 Edit the necessary parameters.
- 6 Optional. If you edited the regular expression, click **Test** to test the regular expression against the payload.
- 7 Click **Save**.

Deleting a custom property

You can delete any custom property, provided the custom property is not associated with another custom property.

- 1 From the **Search** list box, select **Edit Search**.
- 2 Click **Manage Custom Properties**.
- 3 Select the custom property that you want to delete and click **Delete**.
- 4 Click **Yes**.

9 Rule management

Rule permission considerations
Rules overview
Viewing rules
Creating a custom rule
Creating an anomaly detection rule
Rule management tasks
Rule group management
Editing building blocks
Rule page parameters
Rules page toolbar
Rule Response page parameters

From the **Log Activity** tab, you can view and maintain rules.

This topic applies to users who have the **View Custom Rules** or **Maintain Custom Rules** user role permissions.

Rule permission considerations

You can view and manage rules for areas of the network that you can access if you have the **View Custom Rules** and **Maintain Custom Rules** user role permissions.

To create anomaly detection rules, you must have the appropriate **Maintain Custom Rule** permission for tab on which you want create the rule. For example, to be able to create an anomaly detection rule on the **Log Activity** tab, you must have the **Log Activity > Maintain Custom Rule**.

For more information about user role permissions, see the *Extreme Networks Security Log Manager Administration Guide*.

Rules overview

Rules perform tests on events and if all the conditions of a test are met, the rule generates a response.

The tests in each rule can also reference other building blocks and rules. You are not required to create rules in any specific order because the system checks for dependencies each time a new rule is added, edited, or deleted. If a rule that is referenced by another rule is deleted or disabled, a warning is displayed and no action is taken.

For a complete list of default rules, see the *Extreme Networks SIEM Administration Guide*.

Event rule

An event rule performs tests on events as they are processed in real time by the Event processor.

You can create an event rule to detect a single event, within certain properties, or event sequences. For example, if you want to monitor your network for unsuccessful login attempts, access multiple hosts, or a reconnaissance event followed by an exploit, you can create an event rule. It is common for event rules to create offenses as a response.

Rule conditions

Each rule might contain functions, building blocks, or tests.

With functions, you can use building blocks and other rules to create a multi-event function. You can connect rules using functions that support Boolean operators, such as OR and AND. For example, if you want to connect event rules, you can use when an event matches any/all of the following rules function.

A building block is a rule without a response and is used as a common variable in multiple rules or to build complex rules or logic that you want to use in other rules. You can save a group of tests as building blocks for use with other functions. Building blocks will allow you to reuse specific rule tests in other rules. For example, you can save a building block that includes the IP addresses of all mail servers in your network and then use that building block to exclude those mail servers from another rule. The default building blocks are provided as guidelines, which should be reviewed and edited based on the needs of your network.



Note

Building blocks are not loaded by default. Define a rule to build building blocks.

You can run tests on the property of an event such as source IP address or severity of event.

Domain-specific rules

If a rule has a domain test, you can restrict that rule so that it is applied only to events that are happening within a specified domain. An event that has a domain tag that is different from the domain that is set on the rule does not trigger an event response.

To create a rule that tests conditions on things that are happening across the entire system, set the domain condition to **Any Domain**.

Rule responses

When rule conditions are met, a rule can generate one or more responses.

Rules can generate one or more of the following responses:

- Create an offense.
- Send an email.
- Generate system notifications on the Dashboard feature.
- Add data to reference sets.
- Add data to reference data collections.

- Generate a response to an external system.
- Add data to reference data collections that can be used in rule tests.

Reference data collection types

Before you can configure a rule response to send data to a reference data collection, you must create the reference data collection by using the command line interface (CLI). Extreme Security supports the following data collection types:

Reference set	A set of elements, such as a list of IP addresses or user names, that are derived from events and flows occurring on your network.
Reference map	Data is stored in records that map a key to a value. For example, to correlate user activity on your network, you can create a reference map that uses the <i>Username</i> parameter as a key and the user's <i>Global ID</i> as a value.
Reference map of sets	Data is stored in records that map a key to multiple values. For example, to test for authorized access to a patent, use a custom event property for <i>Patent ID</i> as the key and the <i>Username</i> parameter as the value. Use a map of sets to populate a list of authorized users.
Reference map of maps	Data is stored in records that map one key to another key, which is then mapped to single value. For example, to test for network bandwidth violations, you can create a map of maps. Use the <i>Source IP</i> parameter as the first key, the <i>Application</i> parameter as the second key, and the <i>Total Bytes</i> parameter as the value.
Reference table	In a reference table, data is stored in a table that maps one key to another key, which is then mapped to single value. The second key has an assigned type. This mapping is similar to a database table where each column in the table is associated with a type. For example, you can create a reference table that stores the <i>Username</i> parameter as the first key, and has multiple secondary keys that have a user-defined assigned type such as IP Type with the <i>Source IP</i> or <i>Source Port</i> parameter as a value. You can configure a rule response to add one or more keys defined in the table. You can also add custom values to the rule response. The custom value must be valid for the secondary key's type.



Note

For information about reference sets and reference data collections, see the *Administration Guide* for your product.

Viewing rules

You can view the details of a rule, including the tests, building blocks, and responses.

Depending on your user role permissions, you can access the rules page from **Log Activity** tab. For more information about user role permissions, see the *Extreme Networks Security Log Manager Administration Guide*.

The **Rules page** displays a list of rules with their associated parameters. To locate the rule you want to open and view the details of, you can use the Group list box or **Search Rules** field on the toolbar.

- 1 Click the **Log Activity** tab, and then select **Rules** from the **Rules** list box on the toolbar.
- 2 From the **Display** list box, select **Rules**.
- 3 Double-click the rule that you want to view.
- 4 Review the rule details.

If you have the **View Custom Rules** permission, but do not have the **Maintain Custom Rules** permission, the **Rule Summary** page is displayed and the rule cannot be edited. If you have the **Maintain Custom Rules** permission, the **Rule Test Stack Editor** page is displayed. You can review and [edit the rule details](#).

Creating a custom rule

You can create new rules to meet the needs of your deployment.

To create a new rule, you must have the **Offenses > Maintain Custom Rules** permission.

You can test rules locally or globally. A local test means that rule is tested on the local Event processor and not shared with the system. A global test means that the rule is shared and tested by any Event processor on the system. Global rules send events and flows to the central Event processor, which might decrease performance on the central Event processor.

- 1 Click the **Log Activity** tab.
- 2 On the toolbar, click **Rules**.
- 3 From the **Actions** list, select **New Event Rule**.
- 4 Read the introductory text on the Rule wizard. Click **Next**.
- 5 Click **Next** to view the **Rule Test Stack Editor** page.
- 6 In the **enter rule name here** field in the Rule pane, type a unique name that you want to assign to this rule.
- 7 From the list box, select **Local** or **Global**.
- 8 Add one or more tests to a rule:
 - a Optional. To filter the options in the **Test Group** list box, type the text that you want to filter for in the **Type to filter** field.
 - b From the **Test Group** list box, select the type of test you want to add to this rule.
 - c For each test you want to add to the rule, select the plus (+) sign beside the test.
 - d Optional. To identify a test as excluded test, click **and** at the beginning of the test in the Rule pane.
The **and** is displayed as **and not**.
 - e Click the underlined configurable parameters to customize the variables of the test.
 - f From the dialog box, select values for the variable, and then click **Submit**.
- 9 To export the configured rule as a building block to use with other rules:
 - a Click **Export as Building Block**.
 - b Type a unique name for this building block.
 - c Click **Save**.
- 10 On the Groups pane, select the check boxes of the groups to which you want to assign this rule.
- 11 In the **Notes** field, type a note that you want to include for this rule. Click **Next**.
- 12 On the **Rule Responses** page, configure the responses that you want this rule to generate.
- 13 Click **Next**.
- 14 Review the **Rule Summary** page to ensure that the settings are correct. Make changes if necessary, and then click **Finish**.

Creating an anomaly detection rule

Use the Anomaly Detection Rule wizard to create rules that apply time range criteria by using Data and Time tests.

To create a new anomaly detection rule, you must meet the following requirements:

- Have the Maintain Custom Rules permission.
- Perform a grouped search.

The anomaly detection options display after you perform a grouped search and save the search criteria.

You must have the appropriate role permission to be able to create an anomaly detection rule.

To create anomaly detection rules on the **Log Activity** tab, you must have the **Log Activity Maintain Custom Rules** role permission.

To create anomaly detection rules on the **Network Activity** tab, you must have the **Network Maintain Custom Rules** role permission.

Anomaly detection rules use all grouping and filter criteria from the saved search criteria the rule is based on, but do not use any time ranges from the search criteria.

When you create an anomaly detection rule, the rule is populated with a default test stack. You can edit the default tests or add tests to the test stack. At least one Accumulated Property test must be included in the test stack.

By default, the **Test the [Selected Accumulated Property] value of each [group] separately** option is selected on the **Rule Test Stack Editor** page.

This causes an anomaly detection rule to test the selected accumulated property for each event group separately. For example, if the selected accumulated value is **UniqueCount(sourceIP)**, the rule tests each unique source IP address for each event group.

This **Test the [Selected Accumulated Property] value of each [group] separately** option is dynamic. The **[Selected Accumulated Property]** value depends on what option you select for the **this accumulated property test** field of the default test stack. The **[group]** value depends on the grouping options that are specified in the saved search criteria. If multiple grouping options are included, the text might be truncated. Move your mouse pointer over the text to view all groups.

- 1 Click the **Log Activity** tab.
- 2 Perform a search.
- 3 From the **Rules** menu, select the rule type that you want to create. Options include:
 - Add Anomaly Rule
 - Add Threshold Rule
 - Add Behavioral Rule
- 4 Read the introductory text on the Rule wizard. Click **Next**.
The rule that you previously choose is selected.
- 5 Click **Next** to view the **Rule Test Stack Editor** page.
- 6 In the **enter rule name here** field, type a unique name that you want to assign to this rule.

- 7 To add a test to a rule:
 - a Optional. To filter the options in the Test Group list box, type the text that you want to filter for in the Type to filter field.
 - b From the Test Group list box, select the type of test you want to add to this rule.
 - c For each test you want to add to the rule, select the + sign beside the test.
 - d Optional. To identify a test as excluded test, click and at the beginning of the test in the Rule pane. The and is displayed as and not.
 - e Click the underlined configurable parameters to customize the variables of the test.
 - f From the dialog box, select values for the variable, and then click **Submit**.
- 8 Optional. To test the total selected accumulated properties for each event or flow group, clear the **Test the [Selected Accumulated Property] value of each [group] separately** check box.
- 9 In the groups pane, select the check boxes of the groups you want to assign this rule to. For more information, see [Rule group management](#).
- 10 In the **Notes** field, type any notes that you want to include for this rule. Click **Next**.
- 11 On the **Rule Responses** page, configure the responses that you want this rule to generate. [Rule Response page parameters](#) on page 93
- 12 Click **Next**.
- 13 Review the configured rule. Click **Finish**.

Rule management tasks

You can manage custom and anomaly rules.

You can enable and disable rules, as required. You can also edit, copy, or delete a rule.

You can create anomaly detection rules only on the **Log Activity** tab.

Enabling and disabling rules

When you tune your system, you can enable or disable the appropriate rules to ensure that your system generates meaningful offenses for your environment.

You must have the **Log Activity > Maintain Custom Rules** role permission to be able to enable or disable a rule.

- 1 Click the **Log Activity** tab.
- 2 On the toolbar, click **Rules**.
- 3 From the **Display** list box on the **Rules** page, select **Rules**.
- 4 Select the rule that you want to enable or disable.
- 5 From the **Actions** list box, select **Enable/Disable**.

Editing a rule

You can edit a rule to change the rule name, rule type, tests, or responses.

You must have the **Log Activity > Maintain Custom Rules** role permission to be able to enable or disable a rule.

- 1 Click the **Log Activity** tab.
- 2 On the toolbar, click **Rules**.
- 3 From the **Display** list box on the **Rules** page, select **Rules**.
- 4 Double-click the rule that you want to edit.
- 5 From the **Actions** list box, select **Open**.
- 6 Optional. If you want to change the rule type, click **Back** and select a new rule type.
- 7 On the **Rule Test Stack Editor** page, [edit the parameters](#).
- 8 Click **Next**.
- 9 On the **Rule Response** page, [edit the parameters](#).
- 10 Click **Next**.
- 11 Review the edited rule. Click **Finish**.

Copying a rule

You can copy an existing rule, enter a new name for the rule, and then customize the parameters in the new rule as required.

You must have the **Log Activity > Maintain Custom Rules** role permission to be able to enable or disable a rule.

- 1 Click the **Log Activity** tab.
- 2 On the toolbar, click **Rules**.
- 3 From the **Display** list box, select **Rules**.
- 4 Select the rule that you want to duplicate.
- 5 From the **Actions** list box, select **Duplicate**.
- 6 In the Enter name for the copied rule field, type a name for the new rule. Click **OK**.

Deleting a rule

You can delete a rule from your system.

You must have the **Log Activity > Maintain Custom Rules** role permission to be able to enable or disable a rule.

- 1 Click the **Log Activity** tab.
- 2 On the toolbar, click **Rules**.
- 3 From the **Display** list box, select **Rules**.
- 4 Select the rule that you want to delete.
- 5 From the **Actions** list box, select **Delete**.

Rule group management

If you are an administrator, you are able to create, edit, and delete groups of rules. Categorizing your rules or building blocks into groups allows you to efficiently view and track your rules.

For example, you can view all rules that are related to compliance.

As you create new rules, you can assign the rule to an existing group. For information about assigning a group using the rule wizard, see [Creating a custom rule](#) or [Creating an anomaly detection rule](#).

Viewing a rule group

On the **Rules** page, you can filter the rules or building blocks to view only the rules or building blocks that belong to a specific group.

- 1 Click the **Log Activity** tab.
- 2 On the toolbar, click **Rules**.
- 3 From the **Display** list box, select whether you want to view rules or building blocks.
- 4 From the **Filter** list box, select the group category that you want to view.

Creating a group

The **Rules** page provides default rule groups, however, you can create a new group.

- 1 Click the **Log Activity** tab.
- 2 On the toolbar, click **Rules**.
- 3 Click **Groups**.
- 4 From the navigation tree, select the group under which you want to create a new group.
- 5 Click **New Group**.
- 6 Enter values for the following parameters:
 - **Name** - Type a unique name to assign to the new group. The name can be up to 255 characters in length.
 - **Description** - Type a description that you want to assign to this group. The description can be up to 255 characters in length.
- 7 Click **OK**.
- 8 Optional. To change the location of the new group, click the new group and drag the folder to the new location in your navigation tree.

Assigning an item to a group

You can assign a selected rule or building block to a group.

- 1 Click the **Log Activity** tab.
- 2 On the toolbar, click **Rules**.
- 3 Select the rule or building block you want to assign to a group.
- 4 From the **Actions** list box, select **Assign Groups**.
- 5 Select the group that you want to assign the rule or building block to.
- 6 Click **Assign Groups**.
- 7 Close the **Choose Groups** window.

Editing a group

You can edit a group to change the name or description.

- 1 Click the **Log Activity** tab.
- 2 On the toolbar, click **Rules**.
- 3 Click **Groups**.
- 4 From the navigation tree, select the group that you want to edit.
- 5 Click **Edit**.
- 6 Update values for the following parameters:
 - **Name** - Type a unique name to assign to the new group. The name can be up to 255 characters in length.
 - **Description** - Type a description that you want to assign to this group. The description can be up to 255 characters in length.
- 7 Click **OK**.
- 8 Optional. To change the location of the group, click the new group and drag the folder to the new location in your navigation tree.

Copying an item to another group

You can copy a rule or building block from one group to other groups.

- 1 Click the **Log Activity** tab.
- 2 On the toolbar, click **Rules**.
- 3 Click **Groups**.
- 4 From the navigation tree, select the rule or building block you want to copy to another group.
- 5 Click **Copy**.
- 6 Select the check box for the group you want to copy the rule or building block to.
- 7 Click **Copy**.

Deleting an item from a group

You can delete an item from a group. When you delete an item from a group, the rule or building block is only deleted from group; it remains available on the **Rules** page.

- 1 Click the **Log Activity** tab.
- 2 On the toolbar, click **Rules**.
- 3 Click **Groups**.
- 4 Using the navigation tree, navigate to and select the item you want to delete.
- 5 Click **Remove**.
- 6 Click **OK**.

Deleting a group

You can delete a group. When you delete a group, the rules or building blocks of that group remain available on the **Rules** page.

- 1 Click the **Log Activity** tab.
- 2 On the toolbar, click **Rules**.
- 3 Click **Groups**.
- 4 Using the navigation tree, navigate to and select the group that you want to delete.
- 5 Click **Remove**.
- 6 Click **OK**.

Editing building blocks

You can edit any of the default building blocks to match the needs of your deployment.

A building block is a reusable rule test stack that you can include as a component in other rules.

For example, you can edit the BB:HostDefinition: Mail Servers building block to identify all mail servers in your deployment. Then, you can configure any rule to exclude your mail servers from the rule tests.

- 1 Click the **Log Activity** tab.
- 2 On the toolbar, click **Rules**.
- 3 From the **Display** list box, select **Building Blocks**.
- 4 Double-click the building block that you want to edit.
- 5 Update the building block, as necessary.
- 6 Click **Next**.
- 7 Continue through the wizard. For more information, see [Creating a custom rule](#).
- 8 Click **Finish**.

Rule page parameters

A description of the parameters on the **Rules** page.

The list of deployed rules provides the following information for each rule:

Table 31: Rules page parameters

Parameter	Description
Rule Name	Displays the name of the rule.
Group	Displays the group to which this rule is assigned. For more information about groups, see Rule group management .
Rule Category	Displays the rule category for the rule. Options include Custom Rule and Anomaly Detection Rule.
Rule Type	Displays the rule type.
Enabled	Indicates whether the rule is enabled or disabled. For more information about enabling and disabling rules, see Enabling and disabling rules .

Table 31: Rules page parameters (continued)

Parameter	Description
Response	Displays the rule response, if any. Rule responses include: <ul style="list-style-type: none"> • Dispatch New Event • Email • Log Notification • SNMP • Reference Set • Reference Data • IF-MAP Response For more information about rule responses, see Rule responses .
Event Count	Displays the number of events that are associated with this rule when the rule contributes to an offense.
Origin	Displays whether this rule is a default rule (System) or a custom rule (User).
Creation Date	Specifies the date and time this rule was created.
Modification Date	Specifies the date and time this rule was modified.

Rules page toolbar

You use the **Rules** page toolbar to display rules, building blocks or groups. You can manage rule groups and work with rules.

The **Rules** page toolbar provides the following functions:

Table 32: Rules page toolbar function

Function	Description
Display	From the list box, select whether you want to display rules or building blocks in the rules list.
Group	From the list box, select which rule group you want to be displayed in the rules list.
Groups	Click Groups to manage rule groups .
Actions	Click Actions and select one of the following options: <ul style="list-style-type: none"> • New Event Rule - Select this option to create a new event rule. • Enable/Disable - Select this option to enable or disable selected rules. • Duplicate - Select this option to copy a selected rule. • Edit - Select this option to edit a selected rule. • Delete - Select this option to delete a selected rule. • Assign Groups - Select this option to assign selected rules to rule groups.

Table 32: Rules page toolbar function (continued)

Function	Description
Revert Rule	Click Revert Rule to revert a modified system rule to the default value. When you click Revert Rule , a confirmation window is displayed. When you revert a rule, any previous modifications are permanently removed. To revert the rule and maintain a modified version, duplicate the rule and use the Revert Rule option on the modified rule.
Search Rules	Type your search criteria in the Search Rules field and click the Search Rules icon or press Enter on the keyboard. All rules that match your search criteria are displayed in the rules list. The following parameters are searched for a match with your search criteria: <ul style="list-style-type: none"> • Rule Name • Rule (description) • Notes* • Response The Search Rule feature attempts to locate a direct text string match. If no match is found, the Search Rule feature then attempts a regular expression (regex) match.

Rule Response page parameters

There are parameters for the **Rule Response** page.

The following table provides the **Rule Response** page parameters.

Table 33: Event, Flow, and Common Rule Response page parameters

Parameter	Description
Severity	Select this check box if you want this rule to set or adjust severity. When selected, you can use the list boxes to configure the appropriate severity level.
Credibility	Select this check box if you want this rule to set or adjust credibility. When selected, you can use the list boxes to configure the appropriate credibility level.
Relevance	Select this check box if you want this rule to set or adjust relevance. When selected, you can use the list boxes to configure the appropriate relevance level.
Annotate event	Select this check box if you want to add an annotation to this event and type the annotation you want to add to the event.
Drop the detected event	Select this check box to force an event, which is normally sent to the Magistrate component, to be sent to the Ariel database for reporting or searching.
Dispatch New Event	Select this check box to dispatch a new event in addition to the original event, which is processed like all other events in the system. The Dispatch New Event parameters are displayed when you select this check box. By default, the check box is clear.
Event Name	Type a unique name for the event you want to be displayed on the Log Activity tab.

Table 33: Event, Flow, and Common Rule Response page parameters (continued)



Parameter	Description
Event Description	Type a description for the event. The description is displayed in the Annotations pane of the event details.
Severity	From the list box, select the severity for the event. The range is 0 (lowest) to 10 (highest) and the default is 0. The Severity is displayed in the Annotation pane of the event details.
Credibility	From the list box, select the credibility of the event. The range is 0 (lowest) to 10 (highest) and the default is 10. Credibility is displayed in the Annotation pane of the event details.
Relevance	From the list box, select the relevance of the event. The range is 0 (lowest) to 10 (highest) and the default is 10. Relevance is displayed in the Annotation pane of the event details.
High-Level Category	From the list box, select the high-level event category that you want this rule to use when processing events.
Low-Level Category	From the list box, select the low-level event category that you want this rule to use when processing events.
Email	<p>Select this check box to display the email options.</p> <hr/> <div>  <p>Note To change the Email Locale setting, select System Settings on the Admin tab.</p> </div> <hr/>
Enter email addresses to notify	Type the email address to send notification if this rule generates. Use a comma to separate multiple email addresses.
SNMP Trap	<p>This parameter is only displayed when the SNMP Settings parameters are configured in the system settings.</p> <p>Select this check box to enable this rule to send an SNMP notification (trap).</p> <p>The SNMP trap output includes system time, the trap OID, and the notification data, as defined by the MIB.</p>
Send to Local SysLog	<p>Select this check box if you want to log the event locally. By default, this check box is clear.</p> <hr/> <div>  <p>Note Only normalized events can be logged locally on an appliance. If you want to send raw event data, you must use the Send to Forwarding Destinations option to send the data to a remote syslog host.</p> </div> <hr/>
Send to Forwarding Destinations	<p>This check box is only displayed for Event rules.</p> <p>Select this check box if you want to log the event or flow on a forwarding destination. A forwarding destination is a vendor system, such as SIEM, ticketing, or alerting systems. When you select this check box, a list of forwarding destinations is displayed. Select the check box for the forwarding destination you want to send this event or flow to.</p> <p>To add, edit, or delete a forwarding destination, click the Manage Destinations link.</p>

Table 33: Event, Flow, and Common Rule Response page parameters (continued)

Parameter	Description
Notify	<p>Select this check box if you want events that generate as a result of this rule to be displayed in the System Notifications item on the Dashboard tab.</p> <p>If you enable notifications, configure the Response Limiter parameter.</p>
Add to Reference Set	<p>Select this check box if you want events that are generated as a result of this rule to add data to a reference set.</p> <p>To add data to a reference set:</p> <ol style="list-style-type: none"> Using the first list box, select the data that you want to add. Options include all normalized or custom data. Using the second list box, select the reference that is set to which you want to add the specified data. <p>The Add to Reference Set rule response provides the following functions:</p> <p>Refresh Click Refresh to refresh the first list box to ensure that the list is current.</p> <p>Configure Reference Sets Click Configure Reference Sets to configure the reference set. This option is only available if you have administrative permissions.</p>
Add to Reference Data	<p>Before you can use this rule response, you must create the reference data collection by using the command line interface (CLI). For more information about how to create and use reference data collections, see the <i>Administration Guide</i> for your product.</p> <p>Select this check box if you want events that are generated as a result of this rule to add to a reference data collection. After you select the check box, select one of the following options:</p> <p>Add to a Reference Map Select this option to send data to a collection of single key/multiple value pairs. You must select the key and value for the data record, and then select the reference map that you want to add the data record to.</p> <p>Add to a Reference Map Of Sets Select this option to send data to a collection of key/single value pairs. You must select the key and the value for the data record, and then select the reference map of sets you want to add the data record to.</p> <p>Add to a Reference Map Of Maps Select this option to send data to a collection of multiple key/single value pairs. You must select a key for the first map, a key for the second map, and then the value for the data record. You must also select the reference map of maps you want to add the data record to.</p> <p>Add to a Reference Table Select this option to send data to a collection of multiple key/single value pairs, where a type was assigned to the secondary keys. Select the reference table that you want to add data to, and then select a primary key. Select your inner keys (secondary keys) and their values for the data records.</p>

Table 33: Event, Flow, and Common Rule Response page parameters (continued)

Parameter	Description
Publish on the IF-MAP Server	If the IF-MAP parameters are configured and deployed in the system settings, select this option to publish the event information about the IF-MAP server.
Response Limiter	Select this check box and use the list boxes to configure the frequency in which you want this rule to respond.
Enable Rule	Select this check box to enable this rule.

An SNMP notification might resemble:

```
"Wed Sep 28 12:20:57 GMT 2005, Custom Rule Engine Notification -
Rule 'SNMPTRAPTst' Fired. 172.16.20.98:0 -> 172.16.60.75:0 1, Event Name:
ICMP Destination Unreachable Communication with Destination Host is
Administratively Prohibited, QID: 1000156, Category: 1014, Notes:
Offense description"
```

A syslog output might resemble:

```
Sep 28 12:39:01 localhost.localdomain ECS:
Rule 'Name of Rule' Fired: 172.16.60.219:12642
-> 172.16.210.126:6666 6, Event Name: SCAN SYN FIN, QID:
1000398, Category: 1011, Notes: Event description
```


10 Asset profiles

Vulnerabilities

Assets tab overview

Viewing an asset profile

Adding or editing an asset profile

Searching asset profiles

Saving asset search criteria

Asset search groups

Asset profile management tasks

Research asset vulnerabilities

Assets profile page parameters

Asset profiles provide information about each known asset in your network, including what services are running on each asset.

Asset profile information is used for correlation purposes to help reduce false positives. For example, if a source attempts to exploit a specific service running on an asset, then Extreme Security determines if the asset is vulnerable to this attack by correlating the attack to the asset profile.

Asset profiles are automatically discovered if you have vulnerability assessment (VA) scans configured.

Vulnerabilities

You can use Vulnerability Manager and third-party scanners to identify vulnerabilities.

Third-party scanners identify and report discovered vulnerabilities using external references, such as the Open Source Vulnerability Database (OSVDB), National Vulnerability Database (NVDB), and Critical Watch. Examples of third-party scanners include QualysGuard and nCircle ip360. The OSVDB assigns a unique reference identifier (OSVDB ID) to each vulnerability. External references assign a unique reference identifier to each vulnerability. Examples of external data reference IDs include Common Vulnerability and Exposures (CVE) ID or Bugtraq ID. For more information on scanners and vulnerability assessment, see the *Extreme Networks Security Vulnerability Manager User Guide*.

Vulnerability Manager is a component that you can purchase separately and enable using a license key. Vulnerability Manager is a network scanning platform that provides awareness of the vulnerabilities that exist within the applications, systems, or devices on your network. After scans identify vulnerabilities, you can search and review vulnerability data, remediate vulnerabilities, and rerun scans to evaluate the new level of risk.

When Vulnerability Manager is enabled, you can perform vulnerability assessment tasks on the **Vulnerabilities** tab. From the **Assets** tab, you can run scans on selected assets.

For more information, see the *Extreme Networks Security Vulnerability Manager User Guide*

Assets tab overview

The **Assets** tab provides you with a workspace from which you can manage your network assets and investigate an asset's vulnerabilities, ports, applications, history, and other associations.

Using the **Assets** tab, you can:

- View all the discovered assets.
- Manually add asset profiles.
- Search for specific assets.
- View information about discovered assets.
- Edit asset profiles for manually added or discovered assets.
- Tune false positive vulnerabilities.
- Import assets.
- Print or export asset profiles.
- Discover assets.
- Configure and manage third-party vulnerability scanning.
- Start Extreme Security Vulnerability Manager scans.

For more information about the VA Scan option in the navigation pane, see the *Extreme Networks Security Risk Manager User Guide*.

Asset tab list

The **Asset Profiles** page provides information about ID, IP address, Asset name, Aggregate CVSS score, Vulnerabilities, and Services.

The **Asset Profiles** page provides the following information about each asset:

Table 34: Asset Profile page parameters


Parameter	Description
ID	Displays the Asset ID number of the asset. The Asset ID number is automatically generated when you add an asset profile manually or when assets are discovered by event or vulnerability scans.
IP Address	Displays the last known IP address of the asset.
Asset Name	<p>Displays the given name, NetBios name, DSN name, or MAC address of the asset. If unknown, this field displays the last known IP address.</p> <hr/> <div>  <p>Note These values are displayed in priority order. For example, if the asset does not have a given name, the aggregate NetBios name is displayed.</p> </div> <hr/> <p>If the asset is automatically discovered, this field is automatically populated, however, you can edit the asset name if required.</p>

Table 34: Asset Profile page parameters (continued)

Parameter	Description
Risk Score	<p>Displays the one of the following Common Vulnerability Scoring System (CVSS) scores:</p> <ul style="list-style-type: none"> Coalesced aggregate environmental CVSS score Aggregate temporal CVSS score Aggregate CVSS base score These scores are displayed in priority order. For example, if the coalesced aggregate environmental CVSS score is not available, the aggregate temporal CVSS score is displayed. <p>A CVSS score is an assessment metric for the severity of a vulnerability. You can use CVSS scores to measure how much concern a vulnerability warrants in comparison to other vulnerabilities. The CVSS score is calculated from the following user-defined parameters:</p> <ul style="list-style-type: none"> Collateral Damage Potential Confidentiality Requirement Availability Requirement Integrity Requirement <p>For more information about how to configure these parameters, see Adding or editing an asset profile on page 102.</p> <p>For more information about CVSS, see http://www.first.org/cvss/.</p>
Vulnerabilities	Displays the number of unique vulnerabilities that are discovered on this asset. This value also includes the number of active and passive vulnerabilities.
Services	Displays the number of unique Layer 7 applications that run on this asset.
Last User	Displays the last user associated with the asset.
User Last Seen	Displays the time when the last user associated with the asset was last seen.

Assets tab toolbar

The **Asset Profiles** page toolbar allows you to search, save, add, clear, edit, and perform other actions on assets.

The **Asset Profiles** page toolbar provides the following functions:

Table 35: Asset Profiles page toolbar functions

Function	Description
Search	<p>Click Search to perform advanced searches on assets. Options include:</p> <ul style="list-style-type: none"> New Search- Select this option to create a new asset search. Edit Search - Select this option to edit an asset search. <p>For more information about the search feature, see Searching asset profiles.</p>
Quick Searches	From this list box, you can run previously saved searches. Options are displayed in the Quick Searches list box only when you have saved search criteria that specifies the Include in my Quick Searches option.
Save Criteria	Click Save Criteria to save the current search criteria.
Add Filter	Click Add Filter to add a filter to the current search results.

Table 35: Asset Profiles page toolbar functions (continued)

Function	Description
Add Asset	Click Add Asset to add an asset profile. See Adding or editing an asset profile .
Edit Asset	Click Edit Asset to edit an asset profile. This option is enabled only if you have selected an asset profile from the results list. See Adding or editing an asset profile on page 102.
Actions	Click Actions to perform the following actions: <ul style="list-style-type: none"> • Delete Asset - Select this option to delete the selected asset profiles. See Deleting assets. • Delete Listed - Select this option to delete all asset profiles that are listed in the results list. See Deleting assets. • Import Assets - Select this option to import assets. See Importing asset profiles. • Export to XML - Select this option to export asset profiles in XML format. See Exporting assets. • Export to CSV - Select this option to export asset profiles in CSV format. See Exporting assets. • Print - Select this option to print the asset profiles that are displayed on the page. • The Actions menu is available only if you have administrative privileges.
Clear Filter	After you apply a filter using the Add Filter option, you can click Clear Filter to remove the filter.

Right-click menu options

Right-clicking an asset on the Asset tab displays menus for more event filter information.

On the **Assets** tab, you can right-click an asset to access more event filter information.

Table 36: Right-click menu options

Option	Description
Information	The Information menu provides the following options: <ul style="list-style-type: none"> • DNS Lookup - Searches for DNS entries that are based on the IP address. • WHOIS Lookup - Searches for the registered owner of a remote IP address. The default WHOIS server is whois.arin.net. • Port Scan - Performs a Network Mapper (NMAP) scan of the selected IP address. This option is only available if NMAP is installed on your system. For more information about installing NMAP, see your vendor documentation. • Asset Profile - Displays asset profile information. This menu option is only available when an profile data is acquired actively by a scan. • Search Events - Select the Search Events option to search events that are associated with this IP address.
Run Vulnerability Scan	Select this option to run a Vulnerability Manager scan on the selected asset. This option is displayed only after you install Vulnerability Manager.

Viewing an asset profile

From the asset list on the **Assets** tab, you can select and view an asset profile. An asset profile provides information about each profile.

Asset profile information is automatically discovered through Server Discovery or manually configured. You can edit automatically generated asset profile information.

The **Asset Profile** page provides the information about the asset that is organized into several panes. To view a pane, you can click the arrow (>) on the pane to view more detail or select the pane from the **Display** list box on the toolbar.

The **Asset Profile** page toolbar provides the following functions:

Table 37: Asset Profile page toolbar functions

Options	Description
Return to Asset List	Click this option to return to the asset list.
Display	From the list box, you can select the pane that you want to view on the Asset Profile page. The Asset Summary and Network Interface Summary panes are always displayed. For more information about the parameters that are displayed in each pane, see Assets profile page parameters .
Edit Asset	Click this option to edit the Asset Profile. See Adding or editing an asset profile on page 102.
View Destination Summary	If this asset is the destination of an offense, this option will allow you to view destination summary information.
History	Click History to view event history information for this asset. When you click the History icon, the Event Search window is displayed, pre-populated with event search criteria: You can customize the search parameters, if required. Click Search to view the event history information.
Applications	Click Applications to view application information for this asset. When you click the Applications icon, the Flow Search window is displayed, pre-populated with event search criteria. You can customize the search parameters, if required. Click Search to view the application information.
Search Connections	Click Search Connections to search for connections. The Connection Search window is displayed. This option is only displayed when Extreme Networks Security Risk Manager is been purchased and licensed. For more information, see the <i>Extreme Networks Security Risk Manager User Guide</i> .
View Topology	This option is only displayed when Extreme Networks Security Risk Manager is been purchased and licensed. For more information, see the <i>Extreme Networks Security Risk Manager User Guide</i> .
Actions	From the Actions list, select Vulnerability History . This option is only displayed when Extreme Networks Security Risk Manager is been purchased and licensed. For more information, see the <i>Extreme Networks Security Risk Manager User Guide</i> .

- 1 Click the **Assets** tab.
- 2 On the navigation menu, click **Asset Profiles**
- 3 Double-click the asset that you want to view.
- 4 Use the options on the toolbar to display the various panes of asset profile information. See [Editing an asset profile](#).

- 5 To research the associated vulnerabilities, click each vulnerability in the Vulnerabilities pane. See Table 10-10
- 6 If required, edit the asset profile. See [Editing an asset profile](#).
- 7 Click **Return to Assets List** to select and view another asset, if required.

Adding or editing an asset profile

Asset profiles are automatically discovered and added; however, you might be required to manually add a profile

When assets are discovered using the Server Discovery option, some asset profile details are automatically populated. You can manually add information to the asset profile and you can edit certain parameters.

You can only edit the parameters that were manually entered. Parameters that were system generated are displayed in italics and are not editable. You can delete system generated parameters, if required.

- 1 Click the **Assets** tab.
- 2 On the navigation menu, click **Asset Profiles**.
- 3 Choose one of the following options:
 - To add an asset, click **Add Asset** and type the IP address or CIDR range of the asset in the **New IP Address** field.
 - To edit an asset, double-click the asset that you want to view and click **Edit Asset**.
- 4 Configure the parameters in the MAC & IP Address pane. Configure one or more of the following options:
 - Click the **New MAC Address** icon and type a MAC Address in the dialog box.
 - Click the **New IP Address** icon and type an IP address in the dialog box.
 - If **Unknown NIC** is listed, you can select this item, click the **Edit** icon, and type a new MAC address in the dialog box.
 - Select a MAC or IP address from the list, click the **Edit** icon, and type a new MAC address in the dialog box.
 - Select a MAC or IP address from the list and click the **Remove** icon.
- 5 Configure the parameters in the Names & Description pane. Configure one or more of the following options:

Parameter	Description
DNS	Choose one of the following options: <ul style="list-style-type: none"> • Type a DNS name and click Add. • Select a DNS name from the list and click Edit. • Select a DNS name from the list and click Remove.
NetBIOS	Choose one of the following options: <ul style="list-style-type: none"> • Type a NetBIOS name and click Add. • Select a NetBIOS name from the list and click Edit. • Select a NetBIOS name from the list and click Remove.
Given Name	Type a name for this asset profile.
Location	Type a location for this asset profile.

Parameter	Description
Description	Type a description for the asset profile.
Wireless AP	Type the wireless Access Point (AP) for this asset profile.
Wireless SSID	Type the wireless Service Set Identifier (SSID) for this asset profile.
Switch ID	Type the switch ID for this asset profile.
Switch Port ID	Type the switch port ID for this asset profile.

- 6 Configure the parameters in the Operating System pane:
 - a From the **Vendor** list box, select an operating system vendor.
 - b From the **Product** list box, select the operating system for the asset profile.
 - c From the **Version** list box, select the version for the selected operating system.
 - d Click the **Add** icon.
 - e From the **Override** list box, select one of the following options:
 - **Until Next Scan** - Select this option to specify that the scanner provides operating system information and the information can be temporarily edited. If you edit the operating system parameters, the scanner restores the information at its next scan.
 - **Forever** - Select this option to specify that you want to manually enter operating system information and disable the scanner from updating the information.
 - f Select an operating system from the list.
 - g Select an operating system and click the **Toggle Override** icon.
- 7 Configure the parameters in the CVSS & Weight pane. Configure one or more of the following options:

Parameter	Description
Collateral Damage Potential	<p>Configure this parameter to indicate the potential for loss of life or physical assets through damage or theft of this asset. You can also use this parameter to indicate potential for economic loss of productivity or revenue. Increased collateral damage potential increases the calculated value in the CVSS Score parameter.</p> <p>From the Collateral Damage Potential list box, select one of the following options:</p> <ul style="list-style-type: none"> • None • Low • Low-medium • Medium-high • High • Not defined <p>When you configure the Collateral Damage Potential parameter, the Weight parameter is automatically updated.</p>
Confidentiality Requirement	<p>Configure this parameter to indicate the impact on confidentiality of a successfully exploited vulnerability on this asset. Increased confidentiality impact increases the calculated value in the CVSS Score parameter.</p> <p>From the Confidentiality Requirement list box, select one of the following options:</p> <ul style="list-style-type: none"> • Low • Medium • High • Not defined

Parameter	Description
Availability Requirement	<p>Configure this parameter to indicate the impact to the asset's availability when a vulnerability is successfully exploited. Attacks that consume network bandwidth, processor cycles, or disk space impact the availability of an asset. Increased availability impact increases the calculated value in the CVSS Score parameter.</p> <p>From the Availability Requirement list box, select one of the following options:</p> <ul style="list-style-type: none"> • Low • Medium • High • Not defined
Integrity Requirement	<p>Configure this parameter to indicate the impact to the asset's integrity when a vulnerability is successfully exploited. Integrity refers to the trustworthiness and guaranteed veracity of information. Increased integrity impact increases the calculated value in the CVSS Score parameter.</p> <p>From the Integrity Requirement list box, select one of the following options:</p> <ul style="list-style-type: none"> • Low • Medium • High • Not defined
Weight	<p>From the Weight list box, select a weight for this asset profile. The range is 0 - 10.</p> <p>When you configure the Weight parameter, the Collateral Damage Potential parameter is automatically updated.</p>

- 8 Configure the parameters in the Owner pane. Choose one or more of the following options:

Parameter	Description
Business Owner	Type the name of the business owner of the asset. An example of a business owner is a department manager. The maximum length is 255 characters.
Business Owner Contact	Type the contact information for the business owner. The maximum length is 255 characters.
Technical Owner	Type the technical owner of the asset. An example of a business owner is the IT manager or director. The maximum length is 255 characters.
Technical Owner Contact	Type the contact information for the technical owner. The maximum length is 255 characters.
Technical User	From the list box, select the username that you want to associate with this asset profile. You can also use this parameter to enable automatic vulnerability remediation for Vulnerability Manager. For more information about automatic remediation, see the <i>Extreme Networks Security Vulnerability Manager User Guide</i> .

- 9 Click **Save**.

Searching asset profiles

You can configure search parameters to display only the asset profiles you want to investigate from the **Asset** page on the **Assets** tab.

When you access the **Assets** tab, the **Asset** page is displayed populated with all discovered assets in your network. To refine this list, you can configure search parameters to display only the asset profiles you want to investigate.

From the **Asset Search** page, you can manage Asset Search Groups. For more information about Asset Search Groups. See [Asset search groups](#).

The search feature will allow you to search host profiles, assets, and identity information. Identity information provides more detail about log sources on your network, including DNS information, user logins, and MAC addresses.

Using the asset search feature, you can search for assets by external data references to determine whether known vulnerabilities exist in your deployment.

For example:

You receive a notification that CVE ID: CVE-2010-000 is being actively used in the field. To verify whether any hosts in your deployment are vulnerable to this exploit, you can select **Vulnerability External Reference** from the list of search parameters, select **CVE**, and then type the

2010-000

To view a list of all hosts that are vulnerable to that specific CVE ID.



Note

For more information about OSVDB, see <http://osvdb.org/>. For more information about NVD, see <http://nvd.nist.gov/>.

- 1 Click the **Assets** tab.
- 2 On the navigation menu, click **Asset Profiles**.
- 3 On the toolbar, click **Search > New Search**.
- 4 Choose one of the following options:
 - To load a previously saved search, go to Step 5.
 - To create a new search, go to Step 6.
- 5 Select a previously saved search:
 - a Choose one of the following options:
 - Optional. From the **Group** list box, select the asset search group that you want to display in the **Available Saved Searches** list.
 - From the **Available Saved Searches** list, select the saved search that you want to load.
 - In the **Type Saved Search or Select from List** field, type the name of the search you want to load.
 - b Click **Load**.
- 6 In the Search Parameters pane, define your search criteria:
 - a From the first list box, select the asset parameter that you want to search for. For example, **Hostname**, **Vulnerability Risk Classification**, or **Technical Owner**.
 - b From the second list box, select the modifier that you want to use for the search.
 - c In the entry field, type specific information that is related to your search parameter.
 - d Click **Add Filter**.
 - e Repeat these steps for each filter that you want to add to the search criteria.
- 7 Click **Search**.

You can save your asset search criteria. See [Saving asset search criteria](#).

Saving asset search criteria

On the **Asset** tab, you can save configured search criteria so that you can reuse the criteria. Saved search criteria does not expire.

- 1 Click the **Assets** tab.
- 2 On the navigation menu, click **Asset Profiles**.
- 3 Perform a search. See [Searching asset profiles](#).
- 4 Click **Save Criteria**.
- 5 Enter values for the parameters:

Parameter	Description
Enter the name of this search	Type the unique name that you want to assign to this search criteria.
Manage Groups	Click Manage Groups to manage search groups. For more information, see Asset search groups . This option is only displayed if you have administrative permissions.
Assign Search to Group(s)	Select the check box for the group you want to assign this saved search. If you do not select a group, this saved search is assigned to the Other group by default. For more information, see Asset search groups .
Include in my Quick Searches	Select this check box to include this search in your Quick Search list box, which is on the Assets tab toolbar.
Set as Default	Select this check box to set this search as your default search when you access the Assets tab.
Share with Everyone	Select this check box to share these search requirements with all users.

Asset search groups

Using the **Asset Search Groups** window, you can create and manage asset search groups.

These groups allow you to easily locate saved search criteria on the **Assets** tab.

Viewing search groups

Use the **Asset Search Groups** window to view a list group and subgroups.

From the **Asset Search Groups** window, you can view details about each group, including a description and the date the group was last modified.

All saved searches that are not assigned to a group are in the **Other** group.

The **Asset Search Groups** window displays the following parameters for each group:

Table 38: Asset Search Groups window toolbar functions

Function	Description
New Group	To create a new search group, you can click New Group . See Creating a new search group .
Edit	To edit an existing search group, you can click Edit . See Editing a search group .

Table 38: Asset Search Groups window toolbar functions (continued)

Function	Description
Copy	To copy a saved search to another search group, you can click Copy . See Copying a saved search to another group .
Remove	To remove a search group or a saved search from a search group, select the item that you want to remove, and then click Remove . See Removing a group or a saved search from a group .

- 1 Click the **Assets** tab.
- 2 On the navigation menu, click **Asset Profiles**.
- 3 Select **Search > New Search**.
- 4 Click on **Manage Groups**.
- 5 View the search groups.

Creating a new search group

On the **Asset Search Groups** window, you can create a new search group.

- 1 Click the **Assets** tab.
- 2 On the navigation menu, click **Asset Profiles**.
- 3 Select **Search > New Search**.
- 4 Click **Manage Groups**.
- 5 Select the folder for the group under which you want to create the new group.
- 6 Click **New Group**.
- 7 In the **Name** field, type a unique name for the new group.
- 8 Optional. In the **Description** field, type a description.
- 9 Click **OK**.

Editing a search group

You can edit the **Name** and **Description** fields of a search group.

- 1 Click the **Assets** tab.
- 2 On the navigation menu, click **Asset Profiles**.
- 3 Select **Search > New Search**.
- 4 Click **Manage Groups**.
- 5 Select the group that you want to edit.
- 6 Click **Edit**.
- 7 Type a new name in the **Name** field.
- 8 Type a new description in the **Description** field.
- 9 Click **OK**.

Copying a saved search to another group

You can copy a saved search to another group. You can also copy the saved search to more than one group.

- 1 Click the **Assets** tab.
- 2 On the navigation menu, click **Asset Profiles**.
- 3 Select **Search > New Search**.
- 4 Click **Manage Groups**.
- 5 Select the saved search that you want to copy.
- 6 Click **Copy**.
- 7 On the **Item Groups** window, select the check box for the group you want to copy the saved search to.
- 8 Click **Assign Groups**.

Removing a group or a saved search from a group

You can use the **Remove** icon to remove a search from a group or remove a search group.

When you remove a saved search from a group, the saved search is not deleted from your system. The saved search is removed from the group and automatically moved to the **Other** group.

You cannot remove the following groups from your system:

- Asset Search Groups
- Other

- 1 Click the **Assets** tab.
- 2 On the navigation menu, click **Asset Profiles**.
- 3 Select **Search > New Search**.
- 4 Click **Manage Groups**.
- 5 Select the saved search that you want to remove from the group:
 - Select the saved search that you want to remove from the group.
 - Select the group that you want to remove.

Asset profile management tasks

You can delete, import, and export asset profiles using the Assets tab.

Using the **Assets** tab, you can delete, import, and export asset profiles.

Deleting assets

You can delete specific assets or all listed asset profiles.

- 1 Click the **Assets** tab.
- 2 On the navigation menu, click **Asset Profiles**.
- 3 Select the asset that you want to delete, and then select **Delete Asset** from the **Actions** list box.

- 4 Click **OK**.

Importing asset profiles

You can import asset profile information.

The imported file must be a CSV file in the following format:

```
ip,name,weight,description
```

Where:

- **IP** - Specifies any valid IP address in the dotted decimal format. For example: 192.168.5.34.
- **Name** - Specifies the name of this asset up to 255 characters in length. Commas are not valid in this field and invalidate the import process. For example: WebServer01 is correct.
- **Weight** - Specifies a number from 0 to 10, which indicates the importance of this asset on your network. A value of 0 denotes low importance and 10 is very high.
- **Description** - Specifies a textual description for this asset up to 255 characters in length. This value is optional.

For example, the following entries might be included in a CSV file:

- 192.168.5.34,WebServer01,5,Main Production Web Server
- 192.168.5.35,MailServ01,0,

The import process merges the imported asset profiles with the asset profile information you have currently stored in the system.

- 1 Click the **Assets** tab.
- 2 On the navigation menu, click **Asset Profiles**.
- 3 From the **Actions** list box, select **Import Assets**.
- 4 Click **Browse** to locate and select the CSV file that you want to import.
- 5 Click **Import Assets** to begin the import process.

Exporting assets

You can export listed asset profiles to an Extended Markup Language (XML) or Comma-Separated Value (CSV) file.

- 1 Click the **Assets** tab.
- 2 On the navigation menu, click **Asset Profiles**.
- 3 From the **Actions** list box, select one of the following options:
 - Export to XML
 - Export to CSV
- 4 View the status window for the status of the export process.
- 5 Optional: If you want to use other tabs and pages while the export is in progress, click the **Notify When Done** link.

When the export is complete, the **File Download** window is displayed.

- 6 On the **File Download** window, choose one of the following options:
 - **Open** - Select this option to open the export results in your choice of browser.
 - **Save** - Select this option to save the results to your desktop.
- 7 Click **OK**.

Research asset vulnerabilities

The Vulnerabilities pane on the **Asset Profile** page displays a list of discovered vulnerabilities for the asset.

You can double-click the vulnerability to display more vulnerability details.

The **Research Vulnerability Details** window provides the following details:

Parameter	Description
Vulnerability ID	Specifies the ID of the vulnerability. The Vuln ID is a unique identifier that is generated by Vulnerability Information System (VIS).
Published Date	Specifies the date on which the vulnerability details were published on the OSVDB.
Name	Specifies the name of the vulnerability.
Assets	Specifies the number of assets in your network that have this vulnerability. Click the link to view the list of assets.
Assets, including exceptions	Specifies the number of assets in your network that have vulnerability exceptions. Click the link to view the list of assets.
CVE	Specifies the CVE identifier for the vulnerability. CVE identifiers are provided by the NVDB. Click the link to obtain more information. When you click the link, the NVDB website is displayed in a new browser window.
xforce	Specifies the X-Force identifier for the vulnerability. Click the link to obtain more information. When you click the link, the Internet Security Systems website is displayed in a new browser window.
OSVDB	Specifies the OSVDB identifier for the vulnerability. Click the link to obtain more information. When you click the link, the OSVDB website is displayed in a new browser window.
Plugin Details	Specifies the Extreme Security Vulnerability Manager ID. Click the link to view Oval Definitions, Windows Knowledge Base entries, or UNIX advisories for the vulnerability. This feature provides information on how Extreme Security Vulnerability Manager checks for vulnerability details during a patch scan. You can use it to identify why a vulnerability was raised on an asset or why it was not.

Parameter	Description
CVSS Score Base	<p>Displays the aggregate Common Vulnerability Scoring System (CVSS) score of the vulnerabilities on this asset. A CVSS score is an assessment metric for the severity of a vulnerability. You can use CVSS scores to measure how much concern a vulnerability warrants in comparison to other vulnerabilities.</p> <p>The CVSS score is calculated using the following user-defined parameters:</p> <ul style="list-style-type: none"> • Collateral Damage Potential • Confidentiality Requirement • Availability Requirement • Integrity Requirement <p>For more information about how to configure these parameters, see Adding or editing an asset profile on page 102.</p> <p>For more information about CVSS, see http://www.first.org/cvss/.</p>
Impact	Displays the type of harm or damage that can be expected if this vulnerability is exploited.
CVSS Base Metrics	<p>Displays the metrics that are used to calculate the CVSS base score, including:</p> <ul style="list-style-type: none"> • Access Vector • Access complexity • Authentication • Confidentiality impact • Integrity impact • Availability impact
Description	Specifies a description of the detected vulnerability. This value is only available when your system integrates VA tools.
Concern	Specifies the effects that the vulnerability can have on your network.
Solution	Follow the instructions that are provided to resolve the vulnerability.
Virtual Patching	Displays virtual patch information that is associated with this vulnerability, if available. A virtual patch is a short-term mitigation solution for a recently discovered vulnerability. This information is derived from Intrusion Protection System (IPS) events. If you want to install the virtual patch, see your IPS vendor information.
Reference	<p>Displays a list of external references, including:</p> <ul style="list-style-type: none"> • Reference Type - Specifies the type of reference that is listed, such as an advisory URL or mail post list. • URL - Specifies the URL that you can click to view the reference. <p>Click the link to obtain more information. When you click the link, the external resource is displayed in a new browser window.</p>
Products	<p>Displays a list of products that are associated with this vulnerability.</p> <ul style="list-style-type: none"> • Vendor - Specifies the vendor of the product. • Product - Specifies the product name. • Version - Specifies the version number of the product.

- 1 Click the **Assets** tab.
- 2 On the navigation menu, click **Asset Profiles**.
- 3 Select an asset profile.
- 4 In the Vulnerabilities pane, click the **ID** or **Vulnerability** parameter value for the vulnerability you want to investigate.

Assets profile page parameters

You can find Asset profile page parameter descriptions for the Asset Summary pane, Network Interface pane, Vulnerability pane, Services pane, Packages pane, Windows™ Patches pane, Properties pane, Risk Policies pane, and Products pane.

This reference includes tables that describe the parameters that are displayed in each pane of the **Asset Profile** tab.

Asset Summary pane

You can find Parameter descriptions for the Asset Summary pane that you access from the **Asset Profile** page.

The Asset Summary pane on the **Asset Profile** page provides the following information:

Table 10-8 Asset Summary pane parameters

Parameter	Description
Asset ID	Displays the ID number that is assigned to the asset profile.
IP Address	Displays the last reported IP address of the asset.
MAC Address	Displays the last known MAC address of the asset.
Network	Displays the last reported network that is associated with the asset.
NetBIOS Name	Displays the NetBIOS name of the asset, if known. If the asset has more than one NetBIOS name, this field indicates the number of NetBIOS names. Move your mouse pointer over the value to view a list of associated NetBIOS names.
DNS Name	Displays the IP address or DNS name of the asset, if known. If the asset has more than one DNS name, this field indicates the number of DNS names. Move your mouse pointer over the value to view a list of associated DNS names.
Given Name	Displays the name of the asset. By default, this field is empty. To provide a given name for the asset, edit the asset profile.
Group Name	Displays the last known user group of the asset, if known.
Last User	Displays the last known user of the asset. User information is derived from identity events. If more than one user is associated with this asset, you can click the link to display all users.
Operating System	Displays the operating system that is running on the asset. If the asset has more than one operating system, this field indicates the number of operating systems. Move your mouse pointer over the value to view a list of associated operating systems. You can edit this parameter directly if the Override parameter is specified as Until the Next Scan or Forever .
Weight	Displays the level of importance that is associated with this asset. The range is 0 (Not Important) to 10 (Very Important). By default, this field is empty. To provide a weight for the asset, edit the asset profile.

Parameter	Description
Aggregate CVSS Score	<p>Displays the aggregate Common Vulnerability Scoring System (CVSS) score of the vulnerabilities on this asset. A CVSS score is an assessment metric for the severity of a vulnerability. You can use CVSS scores to measure how much concern a vulnerability warrants in comparison to other vulnerabilities.</p> <p>The CVSS score is calculated using the following user-defined parameters:</p> <ul style="list-style-type: none"> • Collateral Damage Potential • Confidentiality Requirement • Availability Requirement • Integrity Requirement <p>For more information about how to configure these parameters, see Adding or editing an asset profile on page 102.</p> <p>For more information about CVSS, see http://www.first.org/cvss/.</p>
Business Owner	Displays the name of the business owner of the asset. An example of a business owner is a department manager.
Business Owner Contact Info	Displays the contact information for the business owner.
CVSS Collateral Damage Potential	<p>Displays the potential this asset has for collateral damage. This value is included in the formula to calculate the CVSS Score parameter.</p> <p>By default this field is not defined. To provide a location for the asset, edit the asset profile.</p>
Technical Owner	Displays the technical owner of the asset. An example of a technical owner is an IT manager or director.
Technical Owner Contact Info	Displays the contact information of the technical owner.
CVSS Availability	Displays the impact to the asset's availability when a vulnerability is successfully exploited.
Wireless AP	Displays the wireless Access Point (AP) for this asset profile.
Wireless SSID	Displays the wireless Service Set Identifier (SSID) for this asset profile.
CVSS Confidentiality Requirements	Displays the impact on confidentiality of a successfully exploited vulnerability on this asset.
Switch ID	Displays the switch ID for this asset profile.
Switch Port ID	Displays the switch port ID for this asset profile.
CVSS Integrity Requirements	Displays the impact to the asset's integrity when a vulnerability is successfully exploited.
Technical User	Specifies the username that is associated with this asset profile.
Open Services	Displays the number of unique Layer 7 applications that run on this asset profile.
Vulnerabilities	Displays the number of vulnerabilities that are discovered on this asset profile.
Location	Specifies the physical location of the asset. By default, this field is empty. To provide a location for the asset, edit the asset profile.
Asset Description	Specifies a description for this asset. By default, this field is empty. To provide a description for the asset, edit the asset profile.
Extra Data	Specifies any extended information that is based on an event.

Network Interface Summary pane

You can find Parameter descriptions for the Network Interface Summary pane that you access from the **Asset Profile** page.

The Network Interface Summary pane on the **Asset Profile** page provides the following information:

Table 1 Network Interface Summary pane parameters

Parameter	Description
MAC Address	Displays the MAC address of this asset, if known.
IP Address	Displays the IP address that is detected for this MAC address.
Network	Displays the network the IP address is associated with, if known.
Last Seen	Displays the date and time the IP address was last detected on this MAC address.

Vulnerability pane

You can find Parameter descriptions for the Vulnerability pane that you access from the **Asset Profile** page.

The Vulnerability pane on the **Asset Profile** page provides the following information:

Table 39: Vulnerability pane parameters

Parameter	Description
ID	Displays the ID of the vulnerability. The ID is a unique identifier that is generated by Vulnerability Information System (VIS).
Severity	Displays the Payment Security Industry (PCI) severity that is associated to vulnerability.
Risk	Risk level that is associated to vulnerability. Sorting on this column must be by the underlying risk level code
Service	Service that is associated to the vulnerability (as discovered by scan). If only 1 service is associated, then display the service. Otherwise, display Multiple (N) where N indicates to total number of services associated to this vulnerability.
Port	Displays the port number this vulnerability was discovered on. If the vulnerability was discovered on more than one port, this field indicates the number of port numbers. Move your mouse pointer over the value to view a list of port numbers.
Vulnerability	Name or title of this vulnerability.
Details	Specific detailed text that is associated to this vulnerability as determined by scan. If only 1 Detail is associated, then display the text of this Detail. Otherwise, display Multiple (N) where N indicates to total number of Details that are associated to this vulnerability.

Table 39: Vulnerability pane parameters (continued)

Parameter	Description
CVSS Score	<p>Displays the aggregate Common Vulnerability Scoring System (CVSS) score of the vulnerabilities on this asset. A CVSS score is an assessment metric for the severity of a vulnerability. You can use CVSS scores to measure how much concern a vulnerability warrants in comparison to other vulnerabilities.</p> <p>The CVSS score is calculated using the following user-defined parameters:</p> <ul style="list-style-type: none"> • Collateral Damage Potential • Confidentiality Requirement • Availability Requirement • Integrity Requirement <p>For more information about how to configure these parameters, see Adding or editing an asset profile on page 102.</p> <p>For more information about CVSS, see http://www.first.org/cvss/.</p>
Found	Displays the date when this vulnerability was originally found in a scan.
Last seen	Displays the date when this vulnerability was last seen in a scan.

Services pane

You can find Parameter descriptions for the Services pane that you access from the **Asset Profile** page.

The Services pane on the **Asset Profile** page provides the following information:

Table 40: Services pane parameters

Parameter	Description
Service	Displays the name of the open service.
Product	Displays the product that runs on this service, if known.
Port	Displays the port the Layer 7 application was discovered on. If this service has more than one port, this field indicates the number of ports. Move your mouse pointer over the value to view a list of port numbers.
Protocol	Displays a comma-separated list of protocols that are discovered on the port that runs the open service.
Last Seen Passive	Displays the date and time that the open service was last passively seen.
Last Seen Active	Displays the date and time that the open service was last actively seen.
Service Default Ports	Displays a comma-separated list of known ports the Layer 7 application is known to run on.
Vulnerabilities	Displays the number of vulnerabilities that are associated with this open service.

Windows™ Services pane

You can find Parameter descriptions for the Windows™ Services pane that you access from the **Asset Profile** page. The Windows™ Services pane is displayed only when Vulnerability Manager is installed on your system.

The Windows™ Services pane on the **Asset Profile** page provides the following information:

Table 41: Windows™ Services pane parameters

Parameter	Description
Name	Displays the name of the Windows™ service that was actively seen on the asset.
Status	Displays the status of the Windows™ service. Options include: <ul style="list-style-type: none"> • Enabled • Manual • Disabled

Packages pane

You can find Parameter descriptions for the Packages pane that you access from the **Asset Profile** page.

The Packages pane is displayed only when Vulnerability Manager is installed on your system. The Packages pane on the **Asset Profile** page provides the following information:

Table 42: Packages pane parameters

Parameter	Description
Packages	Displays the name of the package that is applied to the asset.
Version	Displays the version of the package that is applied to the asset.
Revision	Displays the revision of the package that is applied to the asset.

Windows™ Patches pane

You can find Parameter descriptions for the Windows™ Patches pane that you access from the **Asset Profile** page.

The Windows™ Patches pane is displayed only when Vulnerability Manager is installed on your system. The Windows™ Patches pane on the **Asset Profile** page provides the following information:

Table 43: Windows™ Patches pane parameters

Parameter	Description
Microsoft KB Number	Displays the Microsoft™ Knowledge Base (KB) number of the Windows™ patch that runs on the asset.
Description	Displays the description of the Windows™ patch.
Bulletin ID	Displays the bulletin ID number of the Windows™ patch.
Vulnerability ID	Displays the vulnerability ID of the Windows™ patch.
CVE-ID	Displays the CVE ID associated with the Windows™ patch. If more than one CVE ID is associated with the Windows™ patch, move your mouse over the Multiple link to display the list of CVE IDs. You can click a CVE ID link to access more information.

Table 43: Windows™ Patches pane parameters (continued)

Parameter	Description
System	Displays the Windows™ system for the patch.
Service Pack	Displays the service pack for the patch.

Properties pane

You can find Parameter descriptions for the Properties pane that you access from the **Asset Profile** page. The Properties pane is displayed only when Vulnerability Manager is installed on your system.

The Properties pane on the **Asset Profile** page provides the following information:

Table 44: Properties pane parameters

Parameter	Description
Name	Displays the name of the configuration property that was actively seen on the asset.
Value	Displays the value for the configuration property.

Risk Policies pane

You can find Parameter descriptions for the Risk Policies pane that you access from the **Asset Profile** page. The Risk Policies pane is displayed only when Vulnerability Manager is installed on your system.

The Risk Policies pane on the **Asset Profile** page provides the following information:

Table 45: Risk Policies pane parameters

Parameter	Description
Policy	Displays the name of the policy that is associated with this asset.
Pass/Fail	Indicates whether the policy has a status of Pass or Fail .
Last Evaluated	Displays the date that this policy was last evaluated.

Products pane

You can find Parameter descriptions for the Products pane that you access from the **Asset Profile** page.

The Products pane on the **Asset Profile** page provides the following information:

Table 46: Products pane parameters

Parameter	Description
Product	Displays the name of the product that runs on the asset.
Port	Displays the port that the product uses.

Table 46: Products pane parameters (continued)

Parameter	Description
Vulnerability	Displays the number of vulnerabilities that are associated with this product.
Vulnerability ID	Displays the vulnerability ID.

11 Report management

Reports tab overview
Creating custom reports
Report management tasks
Report groups

You can use the **Reports** tab to create, edit, distribute, and manage reports.

Detailed, flexible reporting options satisfy your various regulatory standards, such as PCI compliance.

You can create your own custom reports or use a default reports. You can customize and rebrand default reports and distribute these to other users.

The **Reports** tab might require an extended period of time to refresh if your system includes many reports.



Note

If you are running Microsoft™ Exchange Server 5.5, unavailable font characters might be displayed in the subject line of emailed reports. To resolve this, download and install Service Pack 4 of Microsoft™ Exchange Server 5.5. For more information, contact Microsoft™ support.

Timezone considerations

To ensure that the Reports feature uses the correct date and time for reporting data, your session must be synchronized with your timezone.

During the installation and setup of Extreme Security products, the time zone is configured. Check with your administrator to ensure your Extreme Security session is synchronized with your timezone.

Report tab permissions

Administrative users can view all reports that are created by other users.

Non-administrative users can view reports that they created only or reports that are shared by other users.

Report tab parameters

The **Reports** tab displays a list of default and custom reports.

From the **Reports** tab, you can view statistical information about the reports template, perform actions on the report templates, view the generated reports, delete generated content.

If a report does not specify an interval schedule, you must **manually generate the report**.

You can point your mouse over any report to preview a report summary in a tooltip. The summary specifies the report configuration and the type of content the report generates.

Reports tab overview

You can create your own custom reports or use a default reports. You can customize and rebrand default reports and distribute these to other users.

The **Reports** tab might require an extended period of time to refresh if your system includes many reports.



Note

If you are running Microsoft™ Exchange Server 5.5, unavailable font characters might be displayed in the subject line of emailed reports. To resolve this, download and install Service Pack 4 of Microsoft™ Exchange Server 5.5. For more information, contact Microsoft™ support.

Timezone considerations

To ensure that the Reports feature uses the correct date and time for reporting data, your session must be synchronized with your timezone.

During the installation and setup of Extreme Security products, the time zone is configured. Check with your administrator to ensure your Extreme Security session is synchronized with your timezone.

Report tab permissions

Administrative users can view all reports that are created by other users.

Non-administrative users can view reports that they created only or reports that are shared by other users.

Report tab parameters

The **Reports** tab displays a list of default and custom reports.

From the **Reports** tab, you can view statistical information about the reports template, perform actions on the report templates, view the generated reports, delete generated content.

The **Reports** tab provides the following information:

Table 47: Report tab parameters

Parameter	Description
Flag Column	If an error occurred, causing the report generation to fail, the Error icon is displayed in this column.
Report Name	Specifies the report name.
Group	Specifies the group to which this report belongs.

Table 47: Report tab parameters (continued)

Parameter	Description
Schedule	Specifies the frequency with which the report is generated. Reports that specify an interval schedule, when enabled, are automatically generated according to the specified interval. If a report does not specify an interval schedule, you must manually generate the report .
Next Run Time	Specifies the duration of time, in hours and minutes, until the next report is generated.
Last Modification	Specifies the last date that this report was modified.
Owner	Specifies the user that owns the report.
Author	Specifies the user that created the report.
Generated Reports	From this list box, select the date stamp of the generated report that you want to view. When you select the date stamp, the Format parameter displays the available formats for the generated reports . If no reports have been generated, None is displayed.
Formats	Specifies the report formats of the currently selected report in the Generated Reports column. Click the icon for the format you want to view.

You can point your mouse over any report to preview a report summary in a tooltip. The summary specifies the report configuration and the type of content the report generates.

Report tab sort order

By default, reports are sorted by the **Last Modification** column. On the **Reports navigation** menu, reports are sorted by interval schedule.

To filter the report to only display reports of a specific frequency, click the arrow beside the **Report** menu item on the navigation menu and select the group (frequency) folder.

Report tab toolbar

You can use the toolbar to perform a number of actions on reports.

The following table identifies and describes the Reports toolbar options.

Table 48: Report toolbar options

Option	Description
Group	
Manage Groups	Click Manage Groups to manage report groups . Using the Manage Groups feature, you can organize your reports into functional groups. You can share report groups with other users.

Table 48: Report toolbar options (continued)

Option	Description
Actions	<p>Click Actions to perform the following actions:</p> <ul style="list-style-type: none"> • Create - Select this option to create a new report. • Edit - Select this option to edit the selected report. You can also double-click a report to edit the content. • Duplicate - Select this option to duplicate or rename the selected report. • Assign Groups - Select this option to assign the selected report to a report group. • Share - Select this option to share the selected report with other users. You must have administrative privileges to share reports. • Toggle Scheduling - Select this option to toggle the selected report to the Active or Inactive state. • Run Report - Select this option to generate the selected report. To generate multiple reports, hold the Control key and click on the reports you want to generate. • Run Report on Raw Data - Select this option to generate the selected report using raw data. This option is useful when you want to generate a report before the required accumulated data is available. For example, if you want to run a weekly report before a full week has elapsed since you created the report, you can generate the report using this option. • Delete Report - Select this option to delete the selected report. To delete multiple reports, hold the Control key and click on the reports you want to delete. • Delete Generated Content - Select this option to delete all generated content for the selected rows. To delete multiple generated reports, hold the Control key and click on the generate reports you want to delete.
Hide Interactive Reports	Select this check box to hide inactive report templates. The Reports tab automatically refreshes and displays only active reports. Clear the check box to show the hidden inactive reports.
Search Reports	<p>Type your search criteria in the Search Reports field and click the Search Reports icon. A search is run on the following parameters to determine which match your specified criteria:</p> <ul style="list-style-type: none"> • Report Title • Report Description • Report Group • Report Groups • Report Author User Name

Report layout

A report can consist of several data elements and can represent network and security data in various styles, such as tables, line charts, pie charts, and bar charts.

When you select the layout of a report, consider the type of report you want to create. For example, do not choose a small chart container for graph content that displays many objects. Each graph includes a legend and a list of networks from which the content is derived; choose a large enough container to hold the data. To preview how each chart displays a data, see [Graph types](#).

Chart types

When you create a report, you must choose a chart type for each chart you want to include in your report.

The chart type determines how the generated report presents data and network objects. You can chart data with several characteristics and create the charts in a single generated report.

You can use any of the following types of charts:

- **None** - Use this option to display an empty container in the report. This option might be useful for creating white space in your report. If you select the **None** option for any container, no further configuration is required for that container.
- **Asset Vulnerabilities** - Use this chart to view vulnerability data for each defined asset in your deployment. You can generate Asset Vulnerability charts when vulnerabilities have been detected by a VA scan. This chart is available after you install Extreme Networks Security Vulnerability Manager.
- **Vulnerabilities** - The Vulnerabilities option is only displayed when the Extreme Networks Security Vulnerability Manager has been purchased and licensed. For more information, see the *Extreme Networks Security Vulnerability Manager User Guide*.

Graph types

Each chart type supports various graph types you can use to display data.

The following graph types are available for Log Manager reports:

- Line Graph
- Stacked Line Graph
- Bar Graph
- Stacked Bar Graph
- Pie Graph
- Table Graph

To display content in a table, you must design a report with a full page width container.

Creating custom reports

Use the Report wizard to create and customize a new report.

You must have appropriate network permissions to share a generated report with other users.

For more information about permissions, see the *Extreme Networks Security Log Manager Administration Guide*.

The Report wizard provides a step-by-step guide on how to design, schedule, and generate reports.

The wizard uses the following key elements to help you create a report:

- **Layout** - Position and size of each container
- **Container** - Placeholder for the featured content
- **Content** - Definition of the chart that is placed in the container

After you create a report that generates weekly or monthly, the scheduled time must elapse before the generated report returns results. For a scheduled report, you must wait the scheduled time period for the results to build. For example, a weekly search requires seven days to build the data. This search will return results after 7 days.

When you specify the output format for the report, consider that the file size of generated reports can be one to 2 megabytes, depending on the selected output format. PDF format is smaller in size and does not use a large quantity of disk storage space.

- 1 Click the **Reports** tab.
- 2 From the **Actions** list box, select **Create**.
- 3 On the **Welcome to the Report wizard!** window, click **Next**.
- 4 Select one of the following options:

Option	Description
--------	-------------

Manually	By default, the report generates 1 time. You can generate the report as often as you want.
-----------------	--

Hourly	Schedules the report to generate at the end of each hour. The data from the previous hour is used.
---------------	--

From the list boxes, select a time frame to begin and end the reporting cycle. A report is generated for each hour within this time frame. Time is available in half-hour increments. The default is 1:00 a.m. for both the **From** and **To** fields.

Weekly	Schedules the report to generate weekly using the data from the previous week.
---------------	--

Select the day that you want to generate the report. The default is Monday. From the list box, select a time to begin the reporting cycle. Time is available in half-hour increments. The default is 1:00 a.m.

Monthly	Schedules the report to generate monthly using the data from the previous month.
----------------	--

From the list box, select the date that you want to generate the report. The default is the first day of the month. Select a time to begin the reporting cycle. Time is available in half-hour increments. The default is 1:00 a.m.

- 5 In the **Allow this report to generate manually** pane, **Yes** or **No**.
- 6 Configure the layout of your report:
 - a From the **Orientation** list box, select **Portrait** or **Landscape** for the page orientation.
 - b Select one of the six layout options that are displayed on the Report wizard.
 - c Click **Next**.

- 7 Specify values for the following parameters:

Parameter	Values
Report Title	The title can be up to 100 characters in length. Do not use special characters.
Logo	From the list box, select a logo.
Pagination Options	From the list box, select a location for page numbers to display on the report. You can choose not to have page numbers display.
Report Classification	Type a classification for this report. You can type up to 75 characters in length. You can use leading spaces, special characters, and double byte characters. The report classification displays in the header and footer of the report. You might want to classify your report as confidential , highly confidential , sensitive , or internal .

- 8 Configure each container in the report:

- a From the **Chart Type** list box, select a chart type.
- b On the **Container Details** window, configure the chart parameters.



Note

You can also create asset saved searches. From the **Search to use** list box, select your saved search.

- c Click **Save Container Details**.
 - d If you selected more than one container, repeat steps a to c.
 - e Click **Next**.
- 9 Preview the **Layout Preview** page, and then click **Next**.
- 10 Select the check boxes for the report formats you want to generate, and then click **Next**.



Important

Extensible Markup Language is only available for tables.

- 11 Select the distribution channels for your report, and then click **Next**. Options include the following distribution channels:

Option	Description
Report Console	Select this check box to send the generated report to the Reports tab. Report Console is the default distribution channel.
Select the users that should be able to view the generated report.	This option displays after you select the Report Console check box. From the list of users, select the users that you want to grant permission to view the generated reports.
Select all users	This option is only displayed after you select the Report Console check box. Select this check box if you want to grant permission to all users to view the generated reports. You must have appropriate network permissions to share the generated report with other users.
Email	Select this check box if you want to distribute the generated report by email.
Enter the report distribution email address(es)	This option is only displayed after you select the Email check box. Type the email address for each generated report recipient; separate a list of email addresses with commas. The maximum characters for this parameter are 255. Email recipients receive this email from no_reply_reports@qradar.
Include Report as attachment (non-HTML only)	This option is only displayed after you select the Email check box. Select this check box to send the generated report as an attachment.
Include link to Report Console	This option is only displayed after you select the Email check box. Select this check box to include a link to the Report Console in the email.

- 12 On the **Finishing Up** page, enter values for the following parameters.

Option	Description
Report Description	Type a description for this report. The description is displayed on the Report Summary page and in the generated report distribution email.
Please select any groups you would like this report to be a member of	Select the groups to which you want to assign this report. For more information about groups, see Report groups .
Would you like to run the report now?	Select this check box if you want to generate the report when the wizard is complete. By default, the check box is selected.

- 13 Click **Next** to view the report summary.

- 14 On the **Report Summary** page, select the tabs available on the summary report to preview your report configuration.

The report immediately generates. If you cleared the **Would you like to run the report now** check box on the final page of the wizard, the report is saved and generates at the scheduled time. The report title is the default title for the generated report. If you reconfigure a report to enter a new report title, the report is saved as a new report with the new name; however, the original report remains the same.

Report management tasks

You use the Reports tab and the Reports wizard to can manage reports.

You can edit, duplicate, share, and brand reports. You can also delete generated reports.

Editing a report

Using the Report wizard, you can edit any default or custom report to change.

You can use or customize a significant number of default reports. The default **Reports** tab displays the list of reports. Each report captures and displays the existing data.



Note

When you customize a scheduled report to generate manually, select the time span **End Date** before you select the **Start Date**.

- 1 Click the **Reports** tab.
- 2 Double-click the report that you want to customize.
- 3 On the Report wizard, change the parameters to customize the report to generate the content you require.

If you reconfigure a report to enter a new report title, the report is saved as a new report with the new name; however, the original report remains the same.

Viewing generated reports

On the **Reports** tab, an icon is displayed in the **Formats** column if a report has generated content. You can click the icon to view the report.

When a report has generated content, the **Generated Reports** column displays a list box. The list box displays all generated content, which is organized by the time-stamp of the report. The most recent reports are displayed at the top of the list. If a report has no generated content, the **None** value is displayed in the **Generated Reports** column.

Icons representing the report format of the generated report are displayed in the **Formats** column.

Reports can be generated in PDF, HTML, RTF, XML, and XLS formats.



Note

The XML and XLS formats are available only for reports that use a single chart table format (portrait or landscape).

You can view only the reports to which you have been given access from the administrator. Administrative users can access all reports.

If you use the Mozilla Firefox web browser and you select the RTF report format, the Mozilla Firefox web browser starts a new browser window. This new window launch is the result of the Mozilla Firefox web browser configuration and does not affect Extreme Security. You can close the window and continue with your Extreme Security session.

- 1 Click the **Reports** tab.

- 2 From the list box in the **Generated Reports** column, select the time-stamp of report you want to view.
- 3 Click the icon for the format you want to view.

Deleting generated content

When you delete generated content, all reports that have generated from the report template are deleted, but the report template is retained.

- 1 Click the **Reports** tab.
- 2 Select the reports for which you want to delete the generated content.
- 3 From the **Actions** list box, click **Delete Generated Content**.

Manually generating a report

A report can be configured to generate automatically, however, you can manually generate a report at any time.

While a report generates, the Next Run Time column displays one of the three following messages:

- **Generating** - The report is generating.
- **Queued (position in the queue)** - The report is queued for generation. The message indicates the position that the report is in the queue. For example, 1 of 3.
- **(x hour(s) x min(s) y sec(s))** - The report is scheduled to run. The message is a count-down timer that specifies when the report will run next.

You can select the **Refresh** icon to refresh the view, including the information in the **Next Run Time** column.

- 1 Click the **Reports** tab.
- 2 Select the report that you want to generate.
- 3 Click **Run Report**.

After the report generates, you can [view the generated report](#) from the Generated Reports column.

Duplicating a report

To create a report that closely resembles an existing report, you can duplicate the report that you want to model, and then customize it.

- 1 Click the **Reports** tab.
- 2 Select the report that you want to duplicate.
- 3 From the **Actions** list box, click **Duplicate**.
- 4 Type a new name, without spaces, for the report.

You can [customize](#) the duplicated report.

Sharing a report

You can share reports with other users. When you share a report, you provide a copy of the selected report to another user to edit or schedule.

Any updates that the user makes to a shared report does not affect the original version of the report.

You must have administrative privileges to share reports. Also, for a new user to view and access reports, an administrative user must share all the necessary reports with the new user.

You can only share the report with users that have the appropriate access.

- 1 Click the **Reports** tab.
- 2 Select the reports that you want to share.
- 3 From the **Actions** list box, click **Share**.
- 4 From the list of users, select the users with whom you want to share this report.

Branding reports

To brand reports, you can import logos and specific images. To brand reports with custom logos, you must upload and configure the logos before you begin using the Report wizard.

Ensure that the graphic you want to use is 144 x 50 pixels with a white background.

To make sure that your browser displays the new logo, clear your browser cache.

Report branding is beneficial for your enterprise if you support more than one logo. When you upload an image, the image is automatically saved as a Portable Network Graphic (PNG).

When you upload a new image and set the image as your default, the new default image is not applied to reports that have been previously generated. Updating the logo on previously generated reports requires you to manually generate new content from the report.

If you upload an image that is larger in length than the report header can support, the image automatically resizes to fit the header; this is approximately 50 pixels in height.

- 1 Click the **Reports** tab.
- 2 On the navigation menu, click **Branding**.
- 3 Click **Browse** to browse the files that are located on your system.
- 4 Select the file that contains the logo you want to upload. Click **Open**.
- 5 Click **Upload Image**.
- 6 Select the logo that you want to use as the default and click **Set Default Image**.

Report groups

You can sort reports into functional groups. If you categorize reports into groups, you can efficiently organize and find reports.

For example, you can view all reports that are related to Payment Card Industry Data Security Standard (PCIDSS) compliance.

By default, the **Reports** tab displays the list of all reports, however, you can categorize reports into groups such as:

- Compliance
- Executive
- Log Sources
- Network Management
- Security
- VoIP
- Other

When you create a new report, you can assign the report to an existing group or create a new group. You must have administrative access to create, edit, or delete groups.

For more information about user roles, see the *Extreme Networks Security Log Manager Administration Guide*.

Creating a report group

You can create new groups.

- 1 Click the **Reports** tab.
- 2 Click **Manage Groups**.
- 3 Using the navigation tree, select the group under which you want to create a new group.
- 4 Click **New Group**.
- 5 Enter values for the following parameters:
 - **Name** - Type the name for the new group. The name can be up to 255 characters in length.
 - **Description** - Optional. Type a description for this group. The description can be up to 255 characters in length.
- 6 Click **OK**.
- 7 To change the location of the new group, click the new group and drag the folder to the new location on the navigation tree.
- 8 Close the **Report Groups** window.

Editing a group

You can edit a report group to change the name or description.

- 1 Click the **Reports** tab.
- 2 Click **Manage Groups**.
- 3 From the navigation tree, select the group that you want to edit.
- 4 Click **Edit**.
- 5 Update values for the parameters, as necessary:
 - **Name** - Type the name for the new group. The name can be up to 255 characters in length.
 - **Description** - Optional. Type a description for this group. The description can be up to 255 characters in length. This field is optional.
- 6 Click **OK**.

- 7 Close the **Report Groups** window.

Sharing report groups

You can share report groups with other users.

You must have administrative permissions to share a report group with other users.

For more information about permissions, see the *Extreme Networks Security Log Manager Administration Guide*.

You cannot use the Content Management Tool (CMT) to share report groups.

For more information about the CMT, see the *Extreme Networks SIEM Administration Guide*.

On the **Report Groups** window, shared users can see the report group in the report list.

Any updates that the user makes to a shared report group does not affect the original version of the report. Only the owner can delete or modify.

A copy of the report is created when a user duplicates or runs the shared report. The user can edit or schedule reports within the copied report group.

The group sharing option overrides previous report sharing options that were configured for reports in the group.

- 1 Click the **Reports** tab.
- 2 On the **Reports** window, click **Manage Groups**.
- 3 On the **Report Groups** window, select the report group that you want to share and click **Share**.
- 4 On the **Sharing Options** window, select one of the following options.

Option	Description
Default (inherit from parent)	<p>The report group is not shared.</p> <p>Any copied report group or generated report remains in the users report list.</p> <p>Each report in the group is assigned any parent report sharing option that was configured.</p>
Share with Everyone	The report group is shared with all users.
Share with users matching the following criteria...	<p>The report group is shared with specific users.</p> <p>User Roles Select from the list of user roles and press the add icon (+).</p> <p>Security Profiles Select from the list of security profiles and press the add icon (+).</p>

- 5 Click **Save**.

On the **Report Groups** window, shared users see the report group in the report list. Generated reports display content based on security profile setting.

Assign a report to a group

You can use the **Assign Groups** option to assign a report to another group.

- 1 Click the **Reports** tab.
- 2 Select the report that you want to assign to a group.
- 3 From the **Actions** list box, select **Assign Groups**.
- 4 From the **Item Groups** list, select the check box of the group you want to assign to this report.
- 5 Click **Assign Groups**.

Copying a report to another group

Use the **Copy** icon to copy a report to one or more report groups.

- 1 Click the **Reports** tab.
- 2 Click **Manage Groups**.
- 3 From the navigation tree, select the report that you want to copy.
- 4 Click **Copy**.
- 5 Select the group or groups to which you want to copy the report.
- 6 Click **Assign Groups**.
- 7 Close the **Report Groups** window.

Removing a report

Use the **Remove** icon to remove a report from a group.

When you remove a report from a group, the report still exists on the **Reports** tab. The report is not removed from your system.

- 1 Click the **Reports** tab.
- 2 Click **Manage Groups**.
- 3 From the navigation tree, navigate to the folder that contains the report you want to remove.
- 4 From the list of groups, select the report that you want to remove.
- 5 Click **Remove**.
- 6 Click **OK**.
- 7 Close the **Report Groups** window.

A Glossary

A
B
C
D
E
F
G
H
I
K
L
M
N
O
P
Q
R
S
T
V
W

This glossary provides terms and definitions for the [product name] software and products.

The following cross-references are used in this glossary:

- See refers you from a nonpreferred term to the preferred term or from an abbreviation to the spelled-out form.
- See *also* refers you to a related or contrasting term.

For other terms and definitions, see the [Terminology website](#) (opens in new window).

[A](#) on page 134 [B](#) on page 134 [C](#) on page 134 [D](#) on page 135 [E](#) on page 135 [F](#) on page 135 [G](#) on page 136 [H](#) on page 136 [I](#) on page 136 [K](#) on page 137 [L](#) on page 137 [M](#) on page 137 [N](#) on page 138 [O](#) on page 138 [P](#) on page 138 [Q](#) on page 139 [R](#) on page 139 [S](#) on page 139 [T](#) on page 140 [V](#) on page 140 [W](#) on page 140

A

accumulator	A register in which one operand of an operation can be stored and subsequently replaced by the result of that operation.
active system	In a high-availability (HA) cluster, the system that has all of its services running.
Address Resolution Protocol (ARP)	A protocol that dynamically maps an IP address to a network adapter address in a local area network.
administrative share	A network resource that is hidden from users without administrative privileges. Administrative shares provide administrators with access to all resources on a network system.
anomaly	A deviation from the expected behavior of the network.
application signature	A unique set of characteristics that are derived by the examination of packet payload and then used to identify a specific application.
ARP	See Address Resolution Protocol .
ARP Redirect	An ARP method for notifying the host if a problem exists on a network.
ASN	See autonomous system number .
asset	A manageable object that is either deployed or intended to be deployed in an operational environment.
autonomous system number (ASN)	In TCP/IP, a number that is assigned to an autonomous system by the same central authority that assigns IP addresses. The autonomous system number makes it possible for automated routing algorithms to distinguish autonomous systems.

B

behavior	The observable effects of an operation or event, including its results.
bonded interface	See link aggregation .
burst	A sudden sharp increase in the rate of incoming events or flows such that the licensed flow or event rate limit is exceeded.

C

CIDR	See Classless Inter-Domain Routing .
Classless Inter-Domain Routing (CIDR)	A method for adding class C Internet Protocol (IP) addresses. The addresses are given to Internet Service Providers (ISPs) for use by their customers. CIDR addresses reduce the size of routing tables and make more IP addresses available within organizations.
client	A software program or computer that requests services from a server.
cluster virtual IP address	An IP address that is shared between the primary or secondary host and the HA cluster.
coalescing interval	The interval at which events are bundled. Event bundling occurs in 10 second intervals and begins with the first event that does not match any currently coalescing events. Within the coalescing interval, the first three matching events are bundled and sent to the event processor.
Common Vulnerability Scoring System (CVSS)	A scoring system by which the severity of a vulnerability is measured.

console	A display station from which an operator can control and observe the system operation.
content capture	A process that captures a configurable amount of payload and then stores the data in a flow log.
credential	A set of information that grants a user or process certain access rights.
credibility	A numeric rating between 0-10 that is used to determine the integrity of an event or an offense. Credibility increases as multiple sources report the same event or offense.
CVSS	See Common Vulnerability Scoring System .

D

database leaf object	A terminal object or node in a database hierarchy.
datapoint	A calculated value of a metric at a point in time.
Device Support Module (DSM)	A configuration file that parses received events from multiple log sources and converts them to a standard taxonomy format that can be displayed as output.
DHCP	See Dynamic Host Configuration Protocol .
DNS	See Domain Name System .
Domain Name System (DNS)	The distributed database system that maps domain names to IP addresses.
DSM	See Device Support Module .
duplicate flow	Multiple instances of the same data transmission received from different flow sources.
Dynamic Host Configuration Protocol (DHCP)	A communications protocol that is used to centrally manage configuration information. For example, DHCP automatically assigns IP addresses to computers in a network.

E

encryption	In computer security, the process of transforming data into an unintelligible form in such a way that the original data either cannot be obtained or can be obtained only by using a decryption process.
endpoint	The address of an API or service in an environment. An API exposes an endpoint and at the same time invokes the endpoints of other services.
external scanning appliance	A machine that is connected to the network to gather vulnerability information about assets in the network.

F

false positive	A test result classed as positive (indicating that the site is vulnerable to attack), that the user decides is in fact negative (not a vulnerability).
flow	A single transmission of data passing over a link during a conversation.
flow log	A collection of flow records.
flow sources	The origin from which flow is captured. A flow source is classified as internal when flow comes from hardware installed on a managed host or it is classified as external when the flow is sent to a flow collector.

forwarding destination	One or more vendor systems that receive raw and normalized data from log sources and flow sources.
FQDN	See fully qualified domain name .
FQNN	See fully qualified network name .
fully qualified domain name (FQDN)	In Internet communications, the name of a host system that includes all of the subnames of the domain name. An example of a fully qualified domain name is rchland.vnet.ibm.com.
fully qualified network name (FQNN)	In a network hierarchy, the name of an object that includes all of the departments. An example of a fully qualified network name is CompanyA.Department.Marketing.

G

gateway A device or program used to connect networks or systems with different network architectures.

H

HA	See high availability .
HA cluster	A high-availability configuration consisting of a primary server and one secondary server.
Hash-Based Message Authentication Code (HMAC)	A cryptographic code that uses a cryptic hash function and a secret key.
high availability (HA)	Pertaining to a clustered system that is reconfigured when node or daemon failures occur so that workloads can be redistributed to the remaining nodes in the cluster.
HMAC	See Hash-Based Message Authentication Code .
host context	A service that monitors components to ensure that each component is operating as expected.

I

ICMP	See Internet Control Message Protocol .
identity	A collection of attributes from a data source that represent a person, organization, place, or item.
IDS	See intrusion detection system .
Internet Control Message Protocol (ICMP)	An Internet protocol that is used by a gateway to communicate with a source host, for example, to report an error in a datagram.
Internet Protocol (IP)	A protocol that routes data through a network or interconnected networks. This protocol acts as an intermediary between the higher protocol layers and the physical network. See also Transmission Control Protocol .
Internet service provider (ISP)	An organization that provides access to the Internet.
intrusion detection system (IDS)	Software that detects attempts or successful attacks on monitored resources that are part of a network or host system.

intrusion prevention system (IPS)	A system that attempts to deny potentially malicious activity. The denial mechanisms could involve filtering, tracking, or setting rate limits.
IP	See Internet Protocol .
IP multicast	Transmission of an Internet Protocol (IP) datagram to a set of systems that form a single multicast group.
IPS	See intrusion prevention system .
ISP	See Internet service provider .

K

key file In computer security, a file that contains public keys, private keys, trusted roots, and certificates.

L

L2L	See Local To Local .
L2R	See Local To Remote .
LAN	See local area network .
LDAP	See Lightweight Directory Access Protocol .
leaf	In a tree, an entry or node that has no children.
Lightweight Directory Access Protocol (LDAP)	An open protocol that uses TCP/IP to provide access to directories that support an X.500 model and that does not incur the resource requirements of the more complex X.500 Directory Access Protocol (DAP). For example, LDAP can be used to locate people, organizations, and other resources in an Internet or intranet directory.
link aggregation	The grouping of physical network interface cards, such as cables or ports, into a single logical network interface. Link aggregation is used to increase bandwidth and network availability.
live scan	A vulnerability scan that generates report data from the scan results based on the session name.
local area network (LAN)	A network that connects several devices in a limited area (such as a single building or campus) and that can be connected to a larger network.
Local To Local (L2L)	Pertaining to the internal traffic from one local network to another local network.
Local To Remote (L2R)	Pertaining to the internal traffic from one local network to another remote network.
log source	Either the security equipment or the network equipment from which an event log originates.
log source extension	An XML file that includes all of the regular expression patterns required to identify and categorize events from the event payload.

M

magistrate	An internal component that analyzes network traffic and security events against defined custom rules.
magnitude	A measure of the relative importance of a particular offense. Magnitude is a weighted value calculated from relevance, severity, and credibility.

N

NAT	See network address translation .
NetFlow	A Cisco network protocol that monitors network traffic flow data. NetFlow data includes the client and server information, which ports are used, and the number of bytes and packets that flow through the switches and routers connected to a network. The data is sent to NetFlow collectors where data analysis takes place.
network address translation (NAT)	In a firewall, the conversion of secure Internet Protocol (IP) addresses to external registered addresses. This enables communications with external networks but masks the IP addresses that are used inside the firewall.
network hierarchy	A type of container that is a hierarchical collection of network objects.
network layer	In OSI architecture, the layer that provides services to establish a path between open systems with a predictable quality of service.
network object	A component of a network hierarchy.
network weight	The numeric value applied to each network that signifies the importance of the network. The network weight is defined by the user.

O

offense	A message sent or an event generated in response to a monitored condition. For example, an offense will provide information on whether a policy has been breached or the network is under attack.
offsite source	A device that is away from the primary site that forwards normalized data to an event collector.
offsite target	A device that is away from the primary site that receives event or data flow from an event collector.
Open Source Vulnerability Database (OSVDB)	Created by the network security community for the network security community, an open source database that provides technical information on network security vulnerabilities.
open systems interconnection (OSI)	The interconnection of open systems in accordance with standards of the International Organization for Standardization (ISO) for the exchange of information.
OSI	See open systems interconnection .
OSVDB	See Open Source Vulnerability Database .

P

parsing order	A log source definition in which the user can define the order of importance for log sources that share a common IP address or host name.
payload data	Application data contained in an IP flow, excluding header and administrative information.
primary HA host	The main computer that is connected to the HA cluster.
protocol	A set of rules controlling the communication and transfer of data between two or more devices or systems in a communication network.

Q

QID Map A taxonomy that identifies each unique event and maps the events to low-level and high-level categories to determine how an event should be correlated and organized.

R

R2L	See Remote To Local .
R2R	See Remote To Remote .
recon	See reconnaissance .
reconnaissance (recon)	A method by which information pertaining to the identity of network resources is gathered. Network scanning and other techniques are used to compile a list of network resource events which are then assigned a severity level.
reference map	A data record of direct mapping of a key to a value, for example, a user name to a global ID.
reference map of maps	A data record of two keys mapped to many values. For example, the mapping of the total bytes of an application to a source IP.
reference map of sets	A data record of a key mapped to many values. For example, the mapping of a list of privileged users to a host.
reference set	A list of single elements that are derived from events or flows on a network. For example, a list of IP addresses or a list of user names.
reference table	A table where the data record maps keys that have an assigned type to other keys, which are then mapped to a single value.
refresh timer	An internal device that is triggered manually or automatically at timed intervals that updates the current network activity data.
relevance	A measure of relative impact of an event, category, or offense on the network.
Remote To Local (R2L)	The external traffic from a remote network to a local network.
Remote To Remote (R2R)	The external traffic from a remote network to another remote network.
report	In query management, the formatted data that results from running a query and applying a form to it.
report interval	A configurable time interval at the end of which the event processor must send all captured event and flow data to the console.
routing rule	A condition that when its criteria are satisfied by event data, a collection of conditions and consequent routing are performed.
rule	A set of conditional statements that enable computer systems to identify relationships and run automated responses accordingly.

S

scanner	An automated security program that searches for software vulnerabilities within web applications.
secondary HA host	The standby computer that is connected to the HA cluster. The secondary HA host assumes responsibility of the primary HA host if the primary HA host fails.
severity	A measure of the relative threat that a source poses on a destination.

Simple Network Management Protocol (SNMP)	A set of protocols for monitoring systems and devices in complex networks. Information about managed devices is defined and stored in a Management Information Base (MIB).
SNMP	See Simple Network Management Protocol .
SOAP	A lightweight, XML-based protocol for exchanging information in a decentralized, distributed environment. SOAP can be used to query and return information and invoke services across the Internet.
standby system	A system that automatically becomes active when the active system fails. If disk replication is enabled, replicates data from the active system.
subnet	See subnetwork .
subnet mask	For internet subnetworking, a 32-bit mask used to identify the subnetwork address bits in the host portion of an IP address.
subnetwork (subnet)	A network that is divided into smaller independent subgroups, which still are interconnected.
sub-search	A function that allows a search query to be performed within a set of completed search results.
superflow	A single flow that is comprised of multiple flows with similar properties in order to increase processing capacity by reducing storage constraints.
system view	A visual representation of both primary and managed hosts that compose a system.

T

TCP	See Transmission Control Protocol .
Transmission Control Protocol (TCP)	A communication protocol used in the Internet and in any network that follows the Internet Engineering Task Force (IETF) standards for internetwork protocol. TCP provides a reliable host-to-host protocol in packet-switched communication networks and in interconnected systems of such networks. See also Internet Protocol .
truststore file	A key database file that contains the public keys for a trusted entity.

V

violation	An act that bypasses or contravenes corporate policy.
vulnerability	A security exposure in an operating system, system software, or application software component.

W

whois server	A server that is used to retrieve information about a registered Internet resources, such as domain names and IP address allocations.
---------------------	---

Index

A

- add asset 98, 102
- add filter 69
- add items 22, 25
- adding event items 25
- adding flow search items 25
- Admin tab 13
- Aggregate CVSS score 98
- anomaly detection rule 86
- Anomaly Detection Rule wizard 86
- asset 99
- Asset name 98
- asset profile 100, 102
- Asset Profile page 110, 112, 114–117
- Asset profile page parameters 112
- asset profiles 97, 106, 109
- Asset profiles 99, 108
- Asset Profiles 107, 108
- Asset profiles page 98
- asset search groups 106
- asset search page 104
- Asset Summary pane parameters 112
- Asset tab 97, 98, 100, 106
- asset vulnerabilities 110
- assets 12, 17, 18
- assets tab 102, 106, 109
- Assets tab 12, 98–100, 107, 108
- assign items to a group 89

B

- browser mode
 - Internet Explorer web browser 11
- building blocks
 - editing 91

C

- calculated property type 76
- calculation property 78
- cancel a search 72
- chart legends 55
- chart objects 55
- chart types 123
- charts overview 53
- configure and manage networks, plug-ins and components 13
- configure and manage systems 13
- configure and manage users 13
- configure page size 18
- configuring charts 55
- configuring connections 23
- configuring dashboard items 23
- configuring log activity 23
- console time 16

- controls 14
- conventions, guide
 - notice icons 6
 - text 7
- copy a rule 88
- copy an item to a group 90
- copy saved search 74, 108
- create a rule group 89
- create new search group 107
- create reports 12
- creating a new search group 74
- creating custom rules 85
- creating search groups 73
- custom event properties 76
- custom property 81
- custom reports 123
- custom rules wizard 14
- Custom Rules Wizard 21

D

- dashboard 25
- dashboard item 25
- dashboard management 19
- dashboard tab 12, 14, 19, 22–24
- Dashboard tab 12, 20
- data searches 57
- default tab 12
- delete a rule 88
- delete asset profile 108
- delete dashboard 24
- deleting a search 73
- deleting assets 108
- detach a dashboard item 24
- disable rules 87
- display in new window 24
- display items 21
- display list box 33
- distribute reports 12
- document mode
 - Internet Explorer web browser 11
- download PCAP data file 41
- download PCAP file 41
- Duplicate a report 128

E

- edit a group 90
- Edit a group 130
- edit a search group 74
- edit asset 102
- edit building blocks 91
- edit search group 107
- enable rules 87
- event description 35
- event details 38

- event details page 35
- event details toolbar 38
- event details toolbar functions 38
- event filter information 100
- event processor results 29
- event rule 83
- event search group 74
- events 20, 39, 55, 57
- export asset profile 108
- exporting assets 109
- exporting events 42

F

- false positives 97
- Flag 21
- flows 55, 57, 62
- functions 83

G

- generate a report manually 128
- glossary 133
- graph types 123
- group
 - assigning items 89
 - copying an item 90
 - deleting 90
 - deleting an item 90
 - editing 90
 - removing 75
- grouped event parameters 33
- grouped events options 33

H

- hosts 12

I

- ID 98
- image
 - reports
 - branding 129
 - upload 129
- import asset profile 108
- import assets 109
- introduction 6
- investigate asset 98
- investigate event logs 12
- investigate log activity 26
- investigating events 20
- IP address 98

L

- last minute (auto refresh) 15
- list of events 35
- log activity

- overview 26
- search criteria 61
- Log Activity dashboard items 20
- log activity tab 15, 28, 29, 31, 33, 39, 40, 42, 57, 71
- Log Activity tab 12, 26
- log source 31

M

- maintain custom rule 82
- maintain custom rules 82
- Manage Groups 108
- manage network 98
- manage reports 12, 121
- manage search results 72, 73
- managing search groups 73
- map event 39
- messages menu 14
- modify event mapping 39
- monitoring events 20
- Most recent reports generated 20
- multiple dashboards 19

N

- navigate Extreme Security 11
- network activity 17, 25, 53, 55, 57, 69
- network activity tab 15, 57
- network administrator 6
- Network Interface pane 112
- Network Interface Summary pane parameters 114
- new features
 - user guide overview 10
- new search 107
- normalized events 29
- notification message 21

O

- offense 39
- offenses 18, 57, 74
- offenses tab 15
- organize your dashboard items 19

P

- Packages pane 112
- Packages pane parameters 116
- Packet Capture (PCAP) data 40
- pause data 15
- PCAP data 40, 41
- PCAP data column 40, 41
- performing a sub-search 69
- permissions
 - custom properties 76
- play data 15
- print asset profile 98
- Products pane 112
- Products pane parameters 117

- properties pane 112
- Properties pane parameters 117
- property
 - copying custom 81
 - modifying custom 79
- property types 76

Q

- QID 39
- quick filter 57

R

- raw event data 31
- real time (streaming) 15
- real-time 29
- refresh data 15
- regex property 77
- regex property type 76
- remove group 75, 108
- Remove icon 108
- remove item from dashboard 23
- remove saved search 108
- remove saved search from a group 75
- rename dashboard 24
- report
 - editing 127
- report groups 131
- Report layout 122
- report tab 120, 121
- report tab parameters 120
- reports
 - viewing 127
- reports tab 15, 120
- Reports tab 12
- resize columns 17
- Rick Policies pane parameters 117
- right-click menu 28
- right-click menu options 100
- Risk Policies pane 112
- rule
 - copying 88
 - edit 87
 - responses 83, 84
- rule group
 - creating 89
 - viewing 89
- rule group management 88
- rule management 82, 87
- rule parameters 91
- rule permission 82
- Rule Response 93
- rules
 - disabling 87
 - enabling 87
 - viewing 84
- rules page toolbar 92

S

- save asset search criteria 106
- save criteria 106
- saving event and flow search criteria 29
- saving search results 71
- scheduled search
 - events 62
 - saved search 62
 - search 62
- search
 - copying to a group 74
- search criteria
 - available saved 70
 - deleting 70
 - log activity tab 70
 - saving 61
- search for asset 98
- search group
 - creating 74
 - editing 74
- search groups
 - managing 73
 - viewing 73
- search groups window 73
- search results
 - cancel 72
 - deleting 73
 - saving 71
 - viewing managed 71
- searching 57
- searching asset profiles 104
- servers 12
- Services 98
- Services pane 112
- Services pane parameters 115
- share reports 129
- sharing report groups 131
- show dashboard 23, 24
- single event details 35
- sort order 121
- sort results in tables 15
- specify chart type 23
- specify number of data objects to view 23
- status bar 29
- streaming events 29
- summary of activity within past 24 hours 20
- synchronize time 120
- system notification 25
- System Notification dashboard item 21
- system notifications 14
- System Summary dashboard item 20
- system time 16

T

- tables 18
- tabs 12
- tests 83

third-party scanners 97
time series chart 54
timezone 120
toolbar 26

U

unparsed event data 31
update user details 17
updated offenses 20
user information 17
user interface 12
user interface tabs 12, 14
user names 16

V

view asset profile 100
view assets 98
view custom rules 82
view grouped events 33
view messages 14
view PCAP data 41
view rule group 89
view system notifications 25
viewing managed search results 71
viewing offenses associated with events 39
viewing search groups 73, 106
viewing streaming events 29
vulnerabilities 97
Vulnerabilities 98
vulnerability details 110
Vulnerability Management dashboard 21
Vulnerability Manager 13, 97
Vulnerability pane 112
Vulnerability pane parameters 114

W

web browser
 supported versions 11
what's new 10
Window Service pane parameters 115
Windows Patches pane parameters 116
Windows Patches pane, 112