



Extreme Networks Security Log Manager Administration Guide

Copyright © 2007–2015 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.....	7
Conventions.....	7
Providing Feedback to Us.....	8
Getting Help.....	9
Related Publications.....	9
Chapter 1: What's new for administrators in Extreme Security V7.2.5.....	11
Chapter 2: Overview of Extreme Security administration.....	13
Supported web browsers.....	13
Admin tab overview.....	14
Deploying changes.....	14
Updating user details.....	15
Monitoring systems with SNMP.....	15
Managing aggregated data views.....	15
RESTful API	16
Chapter 3: User management.....	18
User management overview.....	18
Role management.....	18
Managing security profiles.....	20
User account management.....	23
Authentication management.....	24
User role access and permissions.....	34
Security profile parameters.....	36
User Management window parameters.....	36
User management window toolbar.....	36
User Details window parameters.....	37
Chapter 4: System and licenses management.....	38
System and License Management window overview.....	38
License management checklist.....	40
System management.....	43
Access setting management.....	47
Time server configuration.....	50
Chapter 5: User information source configuration.....	53
User information source overview.....	53
Configuring the Tivoli® Directory Integrator Server.....	56
Creating and managing user information source.....	58
Collecting user information.....	61
Chapter 6: Set up Extreme Security.....	62
Network hierarchy.....	62
Automatic updates.....	65
Set up a Extreme Security update server.....	70
Configuring system settings.....	73
Configuring your IF-MAP server certificates.....	78
SSL certificate replacement in Extreme Security products.....	79
IPv6 addressing in Extreme Security deployments.....	81

Data retention.....	82
Configuring system notifications.....	86
Configuring a custom asset property.....	89
Index management.....	90
Chapter 7: Reference data management.....	92
Adding reference data collections.....	93
Editing reference data collections.....	93
Deleting reference data collections.....	94
Viewing reference data collection contents.....	94
Adding an element to reference data collections.....	95
Deleting elements from reference data collections.....	96
Importing elements into reference data collections.....	96
Exporting elements from reference data collections.....	97
Manage reference data collections with the reference data utility.....	98
Chapter 8: Managing authorized services.....	100
Viewing authorized services.....	100
Adding an authorized service.....	101
Revoking authorized services.....	101
Chapter 9: Manage backup and recovery.....	102
Backup archive management.....	103
Backup archive creation.....	104
Backup archive restoration.....	106
Chapter 10: Deployment editor.....	112
Deployment editor requirements.....	112
Deployment editor views.....	112
Building your deployment using the Deployment Editor.....	114
Generating public keys for Extreme Security products.....	115
Event view management.....	115
Viewing the progress of data rebalancing.....	121
Archiving Data Node content.....	121
Saving event processor data to a Data Node appliance.....	122
System view management.....	122
NAT management.....	129
Component configuration.....	131
Chapter 11: Domain segmentation.....	135
Overlapping IP addresses.....	135
Domain definition and tagging.....	136
Creating domains.....	137
Domain privileges that are derived from security profiles.....	138
Domain-specific rules.....	139
Example: Domain privilege assignments based on custom properties.....	141
Chapter 12: Asset growth deviations.....	143
System notifications for asset growth deviations.....	143
Prevention of asset growth deviations.....	145
Deleting invalid assets.....	153
Deleting blacklist entries.....	153
Modifying asset blacklists and whitelists.....	154

Chapter 13: Configuring QRadar systems to forward data to other systems.....	157
Adding forwarding destinations.....	157
Configuring forwarding profiles.....	158
Configuring routing rules for bulk forwarding.....	159
Configuring selective forwarding.....	160
Viewing forwarding destinations.....	160
Viewing and managing forwarding destinations.....	161
Viewing and managing routing rules.....	161
Chapter 14: Event store and forward	162
Store and forward overview.....	162
Viewing the Store and Forward schedule list.....	163
Creating a new Store and Forward schedule.....	165
Editing a Store and Forward schedule.....	165
Deleting a Store and Forward schedule.....	166
Chapter 15: Content Management Tool overview.....	167
Exporting all custom content.....	168
Exporting all custom content of a specific type.....	169
Searching for content.....	170
Exporting multiple custom content items.....	171
Exporting a single custom content item.....	172
Importing custom content.....	173
Updating content.....	175
Content Management Tool audit details.....	176
Chapter 16: SNMP trap configuration.....	178
Customizing the SNMP trap information sent to another system.....	178
Customizing the SNMP trap output.....	179
Adding a custom SNMP trap to Extreme Security.....	181
Sending SNMP traps to a specific host.....	181
Chapter 17: Data obfuscation.....	183
Generating a private/public key pair.....	184
Configuring data obfuscation.....	186
Decrypting obfuscated data.....	188
Extreme Security asset profile data does not display obfuscated data after upgrade.....	189
Chapter 18: Audit logs.....	190
Viewing the audit log file.....	190
Logged actions.....	191
Chapter 19: Event categories.....	194
High-level event categories.....	194
Recon.....	195
DoS.....	196
Authentication.....	199
Access.....	203
Exploit.....	205
Malware.....	206
Suspicious Activity.....	207
System.....	209

Policy.....	212
Unknown.....	213
CRE.....	214
Potential Exploit.....	214
User Defined.....	215
SIM Audit.....	216
VIS Host Discovery.....	217
Application.....	218
Audit.....	232
Risk.....	233
Risk Manager Audit.....	234
Control.....	234
Asset Profiler.....	236
Chapter 20: Ports used by Extreme Security	239
Searching for ports in use by Extreme Security Console.....	247
Viewing IMQ port associations.....	247
Chapter 21: Extreme Security public servers.....	248
Appendix A: Glossary.....	250
A.....	251
B.....	251
C.....	251
D.....	252
E.....	252
F.....	252
G.....	253
H.....	253
I.....	253
K.....	254
L.....	254
M.....	254
N.....	255
O.....	255
P.....	255
Q.....	256
R.....	256
S.....	256
T.....	257
V.....	257
W.....	257
Index.....	258

About this guide

This guide provides information on managing Extreme Networks Security Log Manager including the Dashboard, Log Activity, and Reports tabs.

Intended audience

This guide is intended for all Extreme Networks Security Log Manager users responsible for investigating and managing network security. This guide assumes that you have Extreme Networks Security Log Manager 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 administrators in Extreme Security V7.2.5

Extreme Networks Security Analytics V7.2.5 introduces domain segmentation, improved LDAP authentication and authorization, centralized log file collection, improved SSH key management, and more features.

Domain segmentation

Extreme Security now supports domain segmentation based on the following input sources: event collectors, log sources, log source groups, and custom properties. You can use security profiles to grant domain privileges and ensure that domain restrictions are respected throughout the entire Extreme Networks Security Analytics system.

 [Learn more...](#)

LDAP authorization

You can use Lightweight Directory Access Protocol (LDAP) providers for authorization. Extreme Security reads the user and role information from the LDAP server, based on the authorization criteria that you defined.

 [Learn more...](#)

Multiple LDAP repositories

You can configure Extreme Security to map entries from multiple LDAP repositories into a single virtual repository.

 [Learn more...](#)

Centralized log file collection

Extreme Security log files contain detailed information about your deployment, such as host names, IP addresses, and email addresses. You can simultaneously collect log files for one or more host systems directly from Extreme Security.

 [Learn more...](#)

Improved SSH key management

SSH keys are now distributed during the Extreme Security deployment. When you upgrade to Extreme Security V7.2.5, the SSH keys that are on the managed hosts are replaced. Removing or altering the

keys might disrupt communication between the Extreme Security Console and the managed hosts, which can result in lost data.

Master Console

Monitor one or multiple Extreme Security deployments with Master Console. You can use Master Console to view system notifications, event and flow rates, CPU usage by process, memory usage, and more operational data.

For more information, see the *IBM Security QRadar Master Console Guide*.

System health

You can now view all of your system notifications, and other health information about your Extreme Security host in one place.

 [Learn more...](#)

Deployment management

You can add managed hosts to your Extreme Security deployment by using Extreme Security management screens within Extreme Security.

The new **Deployment actions** menu gives you the same options as the **Deployment editor**, except for software installations. **Deployment actions** is web-based and doesn't depend on the Java™ client.

 [Learn more...](#)

2 Overview of Extreme Security administration

Supported web browsers
Admin tab overview
Deploying changes
Updating user details
Monitoring systems with SNMP
Managing aggregated data views
RESTful API

Administrators use the **Admin** tab in Extreme Networks Security Analytics to manage dashboards, log activity, assets (if available), and reports.

This overview includes general information on how to access and use the user interface and the **Admin** tab.

Supported web browsers

You access the Extreme Networks Security Analytics console from a standard web browser.

When you access the system, a prompt is displayed asking for a user name and a password. The user name and password must be configured in advance by the administrator.

Table 3: Supported web browsers

Web browser	Supported version
Mozilla Firefox	<ul style="list-style-type: none">• 10.0 ESR• 17.0 ESR <p>Mozilla Firefox has a short release cycle. We cannot commit to testing on the latest versions of the Mozilla Firefox browser. However, we are fully committed to investigating any issues that are reported.</p>
Internet Explorer, with Compatibility View Enabled	<ul style="list-style-type: none">• 8.0• 9.0
Google Chrome	<ul style="list-style-type: none">• Latest version <p>We are fully committed to investigating any issues that are reported.</p>

Admin tab overview

The **Admin** tab provides several tab and menu options that allow you to configure Extreme Security.

You must have administrative privileges to access administrative functions. To access administrative functions, click the **Admin** tab on the user interface.

The **Admin** tab also includes the following menu options:

Table 4: Admin tab menu options

Menu option	Description
Deployment Editor	Opens the Deployment Editor window. For more information, see Deployment editor on page 112.
Deploy Changes	Deploys any configuration changes from the current session to your deployment. For more information, see Deploying changes on page 14.
Advanced	The Advanced menu provides the following options: Deploy Full Configuration - Deploys all configuration changes. When you deploy the full configuration, Extreme Security restarts all services. Data collection for events stops until the deployment completes. For more information, see Deploying changes on page 14.

Deploying changes

You can update your configuration settings from the **Admin** tab. Your changes are saved to a staging area where they are stored until you manually deploy the changes.

Each time that you access the **Admin** tab and each time you close a window on the **Admin** tab, a banner at the top of the **Admin** tab displays the following message: **Checking for undeployed changes**. If undeployed changes are found, the banner updates to provide information about the undeployed changes.

If the list of undeployed changes is lengthy, a scroll bar is provided. Scroll through the list.

The banner message also suggests which type of deployment change to make. Choose one of the two options:

- **Deploy Changes** - Click the **Deploy Changes** icon on the **Admin** tab toolbar to deploy any configuration changes from the current session to your deployment.
- **Deploy Full Configuration** - Select **Advanced > Deploy Full Configuration** from the **Admin** tab menu to deploy all configuration settings to your deployment. All deployed changes are then applied throughout your deployment.

After you deploy your changes, the banner clears the list of undeployed changes and checks the staging area again for any new undeployed changes. If none are present, the following message is displayed: **There are no changes to deploy**.

- 1 Click **View Details**
- 2 Choose one of the following options:
 - a To expand a group to display all items, click the plus sign (+) beside the text. When done, you can click the minus sign (-).

- b To expand all groups, click **Expand All**. When done, you can click **Collapse All**.
 - c Click **Hide Details** to hide the details from view again.
- 3 Perform the suggested task:
 - a From the **Admin** tab menu, click **Deploy Changes**.
 - b From the **Admin** tab menu, click **Advanced > Deploy Full Configuration**.

When you deploy the full configuration, Extreme Security restarts all services. Data collection for events stops until the deployment completes.

Updating user details

You can access your administrative user details through the main user interface.

- 1 Click **Preferences**
- 2 Optional: Update the configurable user details.

Option	Description
Parameter	Description
Email	Type a new email address
Password	Type a new password
Password (Confirm)	Type the new password again
Enable Popup Notifications	Pop-up system notification messages are displayed at the lower right corner of the user interface. To disable pop-up notifications, clear this check box.
	For more information about pop-up notifications, see the <i>User Guide</i> for your product.

- 3 Click **Save**.

Monitoring systems with SNMP

Monitoring of appliances through SNMP polling.

Extreme Networks Security Analytics uses the Net-SNMP agent, which supports various system resource monitoring MIBs. They can be polled by Network Management solutions for the monitoring and alerting of system resources. For more information about Net-SNMP, see Net-SNMP documentation.

Managing aggregated data views

A large volume of data aggregation can decrease system performance. To improve system performance, you can disable, enable, or delete aggregated data views. Time series charts, and report charts use aggregated data views.

The items in the **Display** drop-down list resort the displayed data.

The Aggregate Data View is required to generate data for ADE rules, time series graphs, and reports.

Disable or delete views if the maximum number of views is reached.

Duplicate views can appear in the **Aggregated Data ID** column because an aggregated data view can include multiple searches.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration**.
- 3 Click the **Aggregated Data Management** icon.
- 4 To filter the list of aggregated data views, choose an option from one the following options:
 - Select an option from one of the following lists: **View**, **Database**, **Show**, or **Display**.
 - Type an aggregated data ID, report name, chart name, or saved search name in the search field.
- 5 To manage an aggregated data view, select the view, and then the appropriate action from the toolbar:
 - If you select **Disable View** or **Delete View**, a window displays content dependencies for the aggregated data view. After you disable or delete the aggregated data view, the dependent components no longer use aggregated data.
 - If you enable a disabled aggregated data view, the aggregated data from the deleted view is restored.

Table 5: Aggregated Data Management View column descriptions

Column	Description
Aggregated Data ID	Identifier for the aggregated data
Saved Search Name	Defined name for the saved search
Column Name	Column identifier
Times Searches	Search count
Data Written	The size of the written data
Database Name	Database where the file was written
Last Modified Time	Timestamp of the last data modification
Unique Count Enabled	True or False - search results to display unique event counts instead of average counts over time.

RESTful API

Use the representational state transfer (REST) application programming interface (API) to make HTTPS queries and integrate Extreme Networks Security Analytics with other solutions.

Access and user role permissions

You must have administrative user role permissions in Extreme Security to access and use RESTful APIs. .

Access to the REST API technical documentation user interface

The API user interface provides descriptions and capabilities for the following REST API interfaces:

Table 6: REST API interfaces

REST API	Description
<code>/api/ariel</code>	Query databases, searches, search IDs, and search results.
<code>/api/asset_model</code>	Returns a list of all assets in the model. You can also list all available asset property types and saved searches, and update an asset.
<code>/api/auth</code>	Log out and invalidate the current session.
<code>/api/help</code>	Returns a list of API capabilities.
<code>/api/siem</code>	Returns a list of all offenses.
<code>/api/qvm</code>	Review and manage Extreme Security Vulnerability Manager data.
<code>/api/reference_data</code>	View and manage reference data collections.
<code>/api/qvm</code>	Retrieves assets, vulnerabilities, networks, open services, networks, and filters. You can also create or update remediation tickets.
<code>/api/scanner</code>	View, create, or start a remote scan that is related to a scan profile.

The REST API technical documentation interface provides a framework that you can use to gather the required code that you need to implement Extreme Security functions into other products.

- 1 Enter the following URL in your web browser to access the technical documentation interface:
`https://ConsoleIPAddress/api_doc`.
- 2 Click the header for the API that you want to access, for example, `/ariel`.
- 3 Click the subhead for the endpoint that you want to access, for example, `/databases`.
- 4 Click the Experimental or Provisional sub header.

Note

The API endpoints are annotated as either *experimental* or *stable*.



Experimental

Indicates that the API endpoint might not be fully tested and might change or be removed in the future without any notice.

Stable

Indicates that the API endpoint is fully tested and supported.

- 5 Click **Try it out** to receive properly formatted HTTPS responses.
- 6 Review and gather the information that you need to implement in your third-party solution.

Extreme Security API forum and code samples

The API forum provides more information about the REST API, including the answers to frequently asked questions and annotated code samples that you can use in a test environment. For more information, see the [API forum](#).

3 User management

User management overview
Role management
Managing security profiles
User account management
Authentication management
User role access and permissions
Security profile parameters
User Management window parameters
User management window toolbar
User Details window parameters

Administrators use the **User Management** feature in the **Admin** tab in Extreme Networks Security Analytics to configure and manage user accounts.

When you initially configure Log Manager, you must create user accounts for all users that require access to Log Manager. After initial configuration, you can edit user accounts to ensure that user information is current. You can also add and delete user accounts as required.

User management overview

A user account defines the user name, default password, and email address for a user.

Assign the following items for each new user account that you create:

- **User role** - Determines the privileges that the user is granted to access functions and information in Extreme Security. Two default user roles are defined: Admin and All. Before you add user accounts, you must create more user roles to meet the specific permissions requirement of your users.
- **Security profile** - Determines the networks and log sources the user is granted. Extreme Security includes one default security profile for administrative users. The Admin security profile includes access to all networks and log sources. Before you add user accounts, you must create more security profiles to meet the specific access requirements of your users.

Role management

Using the **User Roles** window, you can create and manage user roles.

Creating a user role

Use this task to create the user roles that are required for your deployment.

By default, your system provides a default administrative user role, which provides access to all areas of Log Manager. Users who are assigned an administrative user role cannot edit their own account. This restriction applies to the default Admin user role. Another administrative user must make any account changes.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration > User Management**.
- 3 Click the **User Roles** icon.
- 4 On the toolbar, click **New**.
- 5 Configure the following parameters:
 - a In the **User Role Name** field, type a unique name for this user role.
 - b Select the permissions that you want to assign to this user role. See [User role access and permissions](#) on page 34.
- 6 In the **Dashboards** area, select the dashboards you want the user role to access, and click **Add**.

Note



- 1 A dashboard displays no information if the user role does not have permission to view dashboard data.
- 2 If a user modifies the displayed dashboards, the defined dashboards for the user role appear at the next login.

- 7 Click **Save**.
- 8 Close the **User Role Management** window.
- 9 On the **Admin** tab menu, click **Deploy Changes**.

Editing a user role

You can edit an existing role to change the permissions that are assigned to the role.

To quickly locate the user role you want to edit on the **User Role Management** window, you can type a role name in the **Type to filter** text box. This box is located above the left pane.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration > User Management**.
- 3 Click the **User Roles** icon.
- 4 In the left pane of the **User Role Management** window, select the user role that you want to edit.
- 5 On the right pane, update the permissions, as necessary. See [User role access and permissions](#) on page 34.
- 6 Modify the **Dashboards** options for the user role as required.
- 7 Click **Save**.
- 8 Close the **User Role Management** window.
- 9 On the **Admin** tab menu, click **Deploy Changes**.

Deleting a user role

If a user role is no longer required, you can delete the user role.

If user accounts are assigned to the user role you want to delete, you must reassign the user accounts to another user role. The system automatically detects this condition and prompts you to update the user accounts.

You can quickly locate the user role that you want to delete on the **User Role Management** window. Type a role name in the **Type to filter** text box, which is located above the left pane.

- 1 Click the **Admin** tab.
- 2 On the **Navigation** menu, click **System Configuration > User Management**.
- 3 Click the **User Roles** icon.
- 4 In the left pane of the **User Role Management** window, select the role that you want to delete.
- 5 On the toolbar, click **Delete**.
- 6 Click **OK**.
 - If user accounts are assigned to this user role, the **Users are Assigned to this User Role** window opens. Go to Step 7.
 - If no user accounts are assigned to this role, the user role is successfully deleted. Go to Step 8.
- 7 Reassign the listed user accounts to another user role:
 - a From the **User Role to assign** list box, select a user role.
 - b Click **Confirm**.
- 8 Close the **User Role Management** window.
- 9 On the **Admin** tab menu, click **Deploy Changes**.

Managing security profiles

Security profiles define which networks and log sources a user can access and the permission precedence.

Using the **Security Profile Management** window, you can view, create, update, and delete security profiles.

Permission precedences

This topic defines each of the permission precedence options.

Permission precedence determines which Security Profile components to consider when the system displays events in the **Log Activity** tab.

Make sure that you understand the following restrictions:

- **No Restrictions** - This option does not place restrictions on which events are displayed in the **Log Activity** tab.
- **Network Only** - This option restricts the user to view only events that are associated with the networks specified in this security profile.
- **Log Sources Only** - This option restricts the user to view only events that are associated with the log sources specified in this security profile.
- **Networks AND Log Sources** - This option allows the user to view only events that are associated with the log sources and networks that are specified in this security profile.

For example, if an event is associated with a log source the security profile allows access to, but the destination network is restricted, the event is not displayed in the **Log Activity** tab. The event must match both requirements.

- **Networks OR Log Sources** - This option allows the user to view only events that are associated with the log sources or networks that are specified in this security profile.

For example, if an event is associated with a log source the security profile allows access to, but the destination network is restricted, the event is displayed in the **Log Activity** tab. The event must match one requirement.

Creating a security profile

To add user accounts, you must first create security profiles to meet the specific access requirements of your users.

Log Manager includes one default security profile for administrative users. The Admin security profile includes access to all networks and log sources.

To select multiple items on the **Security Profile Management** window, hold the Control key while you select each network or network group that you want to add.

If after you add log sources or networks, you want to remove one or more before you save the configuration, you can select the item and click the **Remove (<)** icon. To remove all items, click **Remove All**.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration > User Management**.
- 3 Click the **Security Profiles** icon.
- 4 On the **Security Profile Management** window toolbar, click **New**.
- 5 Configure the following parameters:
 - a In the **Security Profile Name** field, type a unique name for the security profile. The security profile name must meet the following requirements: minimum of 3 characters and maximum of 30 characters.
 - b **Optional** Type a description of the security profile. The maximum number of characters is 255.
- 6 Click the **Permission Precedence** tab.
- 7 In the Permission Precedence Setting pane, select a permission precedence option. See [Permission precedences](#) on page 20.
- 8 Configure the networks that you want to assign to the security profile:
 - a Click the **Networks** tab.
 - b From the navigation tree in the left pane of the **Networks** tab, select the network that you want this security profile to have access to.
 - c Click the **Add (>)** icon to add the network to the Assigned Networks pane.
 - d Repeat for each network you want to add.
- 9 Configure the log sources that you want to assign to the security profile:
 - a Click the **Log Sources** tab.
 - b From the navigation tree in the left pane, select the log source group or log source you want this security profile to have access to.

- c Click the **Add (>)** icon to add the log source to the Assigned Log Sources pane.
- d Repeat for each log source you want to add.
- 10 Click **Save**.
- 11 Close the **Security Profile Management** window.
- 12 On the **Admin** tab menu, click **Deploy Changes**.

Editing a security profile

You can edit an existing security profile to update which networks and log sources a user can access and the permission precedence.

To quickly locate the security profile you want to edit on the **Security Profile Management** window, type the security profile name in the **Type to filter** text box. It is located above the left pane.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration > User Management**.
- 3 Click the **Security Profiles** icon.
- 4 In the left pane, select the security profile you want to edit.
- 5 On the toolbar, click **Edit**.
- 6 Update the parameters as required.
- 7 Click **Save**.
- 8 If the **Security Profile Has Time Series Data** window opens, select one of the following options:

Option	Description
Keep Old Data and Save	Select this option to keep previously accumulated time series data. If you choose this option, issues might occur when users associated with this security profile views time series charts.
Hide Old Data and Save	Select this option to hide the time-series data. If you choose this option, time series data accumulation restarts after you deploy your configuration changes.

- 9 Close the **Security Profile Management** window.
- 10 On the **Admin** tab menu, click **Deploy Changes**.

Duplicating a security profile

If you want to create a new security profile that closely matches an existing security profile, you can duplicate the existing security profile and then modify the parameters.

To quickly locate the security profile you want to duplicate on the **Security Profile Management** window, you can type the security profile name in the **Type to filter** text box, which is located above the left pane.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration User Management**.
- 3 Click the **Security Profiles** icon.
- 4 In the left pane, select the security profile you want to duplicate.
- 5 On the toolbar, click **Duplicate**.
- 6 In the **Confirmation** window, type a unique name for the duplicated security profile.

- 7 Click **OK**.
- 8 Update the parameters as required.
- 9 Close the **Security Profile Management** window.
- 10 On the **Admin** tab menu, click **Deploy Changes**.

Deleting a security profile

If a security profile is no longer required, you can delete the security profile.

If user accounts are assigned to the security profiles you want to delete, you must reassign the user accounts to another security profile. Log Manager automatically detects this condition and prompts you to update the user accounts.

To quickly locate the security profile you want to delete on the **Security Profile Management** window, you can type the security profile name in the **Type to filter** text box. It is located above the left pane.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration > User Management**.
- 3 Click the **Security Profiles** icon.
- 4 In the left pane, select the security profile that you want to delete.
- 5 On the toolbar, click **Delete**.
- 6 Click **OK**.
 - If user accounts are assigned to this security profile, the **Users are Assigned to this Security Profile** window opens. Go to [Deleting a user role](#) on page 19.
 - If no user accounts are assigned to this security profile, the security profile is successfully deleted. Go to [Deleting a user role](#) on page 19.
- 7 Reassign the listed user accounts to another security profile:
 - a From the **User Security Profile to assign** list box, select a security profile.
 - b Click **Confirm**.
- 8 Close the **Security Profile Management** window.
- 9 On the **Admin** tab menu, click **Deploy Changes**.

User account management

This topic provides information about managing user accounts.

When you initially configure your system, you must create user accounts for each of your users. After initial configuration, you might be required to create more user accounts and manage existing user accounts.

Creating a user account

You can create new user accounts.

Before you can create a user account, you must ensure that the required user role and security profile are created.

When you create a new user account, you must assign access credentials, a user role, and a security profile to the user. User Roles define what actions the user has permission to perform. Security Profiles define what data the user has permission to access.

You can create multiple user accounts that include administrative privileges; however, any Administrator Manager user accounts can create other administrative user accounts.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration > User Management**.
- 3 Click the **Users** icon.
- 4 On the **User Management** toolbar, click **New**.
- 5 Enter values for the following parameters:
 - a In the **Username** field, type a unique user name for the new user. The user name must contain a maximum 30 characters.
 - b In the **Password** field, type a password for the user to gain access.
The password must meet the following criteria:
 - Minimum of 5 characters
 - Maximum of 255 characters
- 6 Click **Save**.
- 7 Close the **User Details** window.
- 8 Close the **User Management** window.
- 9 On the **Admin** tab menu, click **Deploy Changes**.

Deleting a user account

If a user account is no longer required, you can delete the user account.

After you delete a user, the user no longer has access to the user interface. If the user attempts to log in, a message is displayed to inform the user that the user name and password is no longer valid. Items that a deleted user created, such as saved searches and reports remain associated with the deleted user.

To quickly locate the user account you want to delete on the **User Management** window, you can type the user name in the **Search User** text box on the toolbar.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration > User Management**.
- 3 Click the **Users** icon.
- 4 Select the user that you want to delete.
- 5 On the toolbar, click **Delete**.
- 6 Click **OK**.
- 7 Close the **User Management** window.

Authentication management

This topic provides information and instructions for how to configure authentication.

Log Manager supports various authentication types. You can configure authentication to validate users and passwords.

Authentication overview

When authentication is configured and a user enters an invalid user name and password combination, a message is displayed to indicate that the login was invalid.

If the user attempts to access the system multiple times with invalid information, the user must wait the configured amount of time before another attempt to access the system again. You can configure Console settings to determine the maximum number of failed logins, and other related settings. For more information about configuring Console settings for authentication, see [Set up Extreme Security](#) on page 62 [Configuring the Console settings](#).

An administrative user can access Log Manager through a vendor authentication module or by using the local Admin password. The Admin password functions if you set up and activated a vendor authentication module. However, you cannot change the Admin password while the authentication module is active. To change the Admin password, you must temporarily disable the vendor authentication module, reset the password, and then reconfigure the vendor authentication module.

Log Manager supports the following user authentication types:

- **System authentication** - Users are authenticated locally. This is the default authentication type.
- **RADIUS authentication** - Users are authenticated by a Remote Authentication Dial-in User Service (RADIUS) server. When a user attempts to log in, Log Manager encrypts the password only, and forwards the user name and password to the RADIUS server for authentication.
- **TACACS authentication** - Users are authenticated by a Terminal Access Controller Access Control System (TACACS) server. When a user attempts to log in, Log Manager encrypts the user name and password, and forwards this information to the TACACS server for authentication. TACACS Authentication uses Cisco Secure ACS Express® as a TACACS server. Log Manager supports up to Cisco Secure ACS Express® 4.3.
- **Active directory** - Users are authenticated by a Lightweight Directory Access Protocol (LDAP) server that uses Kerberos.
- **LDAP** - Users are authenticated by a Native LDAP server.

Authentication type prerequisite tasks checklist

Prerequisite task are required before you configure RADIUS, TACACS, Active Directory, or LDAP as the authentication type.

Before you can configure RADIUS, TACACS, Active Directory, or LDAP as the authentication type, you must complete the following tasks:

- Configure the authentication server before you configure authentication in Log Manager. For more information, see your server documentation
- Ensure that the server has the appropriate user accounts and privilege levels to communicate with Log Manager. For more information, see your server documentation.

- Ensure that the time of the authentication server is synchronized with the time of the Log Manager server. For more information about setting time, see [Set up Extreme Security](#) on page 62.
- Ensure that all users have appropriate user accounts and roles to allow authentication with the vendor servers.

Configuring system authentication

You can configure local authentication on your Extreme Security system.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration > User Management**.
- 3 Click the **Authentication** icon.
- 4 From the **Authentication Module** list box, select the **System Authentication**.
- 5 Click **Save**.

Configuring RADIUS authentication

You can configure RADIUS authentication on your Extreme Security system.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration User Management**.
- 3 Click the **Authentication** icon.
- 4 From the **Authentication Module** list box, select **RADIUS Authentication**.
- 5 Configure the parameters:
 - a In the **RADIUS Server** field, type the host name or IP address of the RADIUS server.
 - b In the **RADIUS Port** field, type the port of the RADIUS server.
 - c From the **Authentication Type** list box, select the type of authentication you want to perform.

Choose from the following options:

Option	Description
CHAP	Challenge Handshake Authentication Protocol (CHAP) establishes a Point-to-Point Protocol (PPP) connection between the user and the server.
MSCHAP	Microsoft™ Challenge Handshake Authentication Protocol (MSCHAP) authenticates remote Windows™ workstations.
ARAP	Apple Remote Access Protocol (ARAP) establishes authentication for AppleTalk network traffic.
PAP	Password Authentication Protocol (PAP) sends clear text between the user and the server.

- d In the **Shared Secret** field, type the shared secret that Log Manager uses to encrypt RADIUS passwords for transmission to the RADIUS server.
- 6 Click **Save**.

Configuring TACACS authentication

You can configure TACACS authentication on your Extreme Security system.

- 1 Click the **Admin** tab.
- 2 On the **navigation** menu, click **System Configuration > User Management**.
- 3 Click the **Authentication** icon.
- 4 From the **Authentication Module** list box, select **TACACS Authentication**.
- 5 Configure the parameters:
 - a In the **TACACS Server** field, type the host name or IP address of the TACACS server.
 - b In the **TACACS Port** field, type the port of the TACACS server.
 - c From the **Authentication Type** list box, select the type of authentication you want to perform.

Choose from the following options:

Option	Description
ASCII	American Standard Code for Information Interchange (ASCII) sends the user name and password in clear, unencrypted text.
PAP	Password Authentication Protocol (PAP) sends clear text between the user and the server. This is the default authentication type.
CHAP	Challenge Handshake Authentication Protocol (CHAP) establishes a Point-to-Point Protocol (PPP) connection between the user and the server.
MSCHAP	Microsoft™ Challenge Handshake Authentication Protocol (MSCHAP) authenticates remote Windows™ workstations.
MSCHAP2	Microsoft™ Challenge Handshake Authentication Protocol version 2 (MSCHAP2) authenticates remote Windows™ workstations using mutual authentication.
EAPMD5	Extensible Authentication Protocol using MD5 Protocol (EAPMD5) uses MD5 to establish a PPP connection.

- d In the **Shared Secret** field, type the shared secret that Extreme Security uses to encrypt TACACS passwords for transmission to the TACACS server.
- 6 Click **Save**.

Configuring Active Directory authentication

You can configure Active Directory authentication on your Extreme Networks Security Analytics system.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration** and then click the **Authentication** icon.
- 3 From the **Authentication Module** list box, select **Active Directory**.

Configure the following parameters:

Parameter	Description
Server URL	Type the URL used to connect to the LDAP server, for example, <code>ldaps://host:port</code> .
LDAP Context	Type the LDAP context you want to use, for example, <code>DC=QRADAR,DC=INC</code> .
LDAP Domain	Type the LDAP context you want to use, for example, <code>DC=QRADAR,DC=INC</code> .
LDAP Domain	Type the domain that you want to use, for example <code>qradar.inc</code> .

- 4 Click **Save**.

LDAP authentication

You can configure Extreme Security to use supported Lightweight Directory Access Protocol (LDAP) providers for user authentication and authorization.

Extreme Security reads the user and role information from the LDAP server, based on the authorization criteria that you defined.

Authentication

Authentication establishes proof of identity for any user who attempts to log in to the Extreme Security server. When a user logs in, the user name and password are sent to the LDAP directory to verify whether the credentials are correct. To send this information securely, configure the LDAP server connection to use Secure Socket Layer (SSL) or Transport Layer Security (TLS) encryption.

Use anonymous bind to create a session with the LDAP directory server that doesn't require that you provide authentication information.

Authenticated bind requires that the session has a valid user name and password combination. A successful authenticated bind authorizes the authenticated user to read the list of users and roles from the LDAP directory during the session.

For increased security, ensure that the user ID that is used for the bind connection does not have permissions to do anything other than reading the LDAP directory.

Authorization

Authorization is the process of determining what access permissions a user has. Users are authorized to perform tasks based on their role assignments.

You must have a valid bind connection to the LDAP server before you can select authorization settings.

Local	The LDAP servers are used only to authenticate users. The user name and password combination is verified for each user that logs in, but no authorization information is exchanged between the LDAP server and Extreme Security server. If you chose Local authorization, you must create each user on the Extreme Security console.
User attributes	Forms a search filter that is used when users are authenticated. You must specify both a user role attribute and a security profile attribute. The attributes that you can use are retrieved from the LDAP server, based on your connection settings.
Group	Users inherit role-based access permissions after they authenticate with the LDAP server. The LDAP group member lists are retrieved based on the attributes that are configured in the Group Member Field . All users in those groups inherit permissions based on what the Extreme Security role allows. You can configure separate groups permit or deny permissions for security profiles and user roles.

User attribute values are case-sensitive. The mapping of group names to user roles and security profiles is also case-sensitive.

Data synchronization

If you use authorization that is based on user attributes or groups, user information is automatically imported from the LDAP server to the Extreme Security console. Each group that is configured on the LDAP server must have a matching user role or security profile that is configured on the Extreme

Security console. For each group that matches, the users are imported and assigned permissions that are based on that user role or security profile.

By default, synchronization happens every 24 hours. The timing for synchronization is based on the last run time. For example, if you manually run the synchronization at 11:45 pm, and set the synchronization interval to 8 hours, the next synchronization will happen at 7:45 am. If the access permissions change for a user that is logged in when the synchronization occurs, the session becomes invalid. The user is redirected back to the login screen with the next request.

To synchronize data manually, follow these steps:

- 1 On the **Admin** tab, click **System Configuration** and then click **Authentication**.
- 2 In the **Authentication Module** list, select **LDAP**.
- 3 Click **Manage Synchronization** and then click **Run Synchronization Now**.

Configuring LDAP authentication

You can configure Extreme Networks Security Analytics system to use SSL encryption or TLS authentication when connecting to the LDAP server.

If you plan to use SSL encryption or use TLS authentication with your LDAP server, you must import the SSL or TLS certificate from the LDAP server to the `/opt/gradar/conf/trusted_certificates` directory on your Extreme Security console. For more information about configuring the certificates, see [Configuring SSL or TLS certificates](#) on page 33.

If you are using group authorization, you must configure a Extreme Security user role or security profile on the Extreme Security console for each LDAP group that is used by Extreme Security. Every Extreme Security user role or security profile must have at least one accept group. The mapping of group names to user roles and security profiles is case-sensitive.

The following table shows the parameters that are required to configure an LDAP authentication provider.

The following table provides configuration information about each of the parameters that are used to configure an LDAP authentication provider.

Table 7: LDAP authentication provider parameters

Parameter	Description
Server URL	The DNS name or IP address of the LDAP server. The URL must include a port value. For example, <code>ldap://<host_name>:<port></code> or <code>ldap://<ip_address>:<port></code> .
SSL connection	If SSL encryption is enabled, the value in the Server URL field must specify a secure connection, for example, <code>ldaps://secureldap.mydomain.com:636</code> .
TLS authentication	Transport Layer Security (TLS) encryption to connect to the LDAP server is negotiated as part of the normal LDAP protocol and does not require a special protocol designation or port in the Server URL field.
Search entire base	Select True to search all subdirectories of the specified Directory Name (DN). Select False to search only the immediate contents of the Base DN. The subdirectories are not searched.

Table 7: LDAP authentication provider parameters (continued)

Parameter	Description
LDAP user field	The user field identifier that you want to search on. You can specify multiple user fields in a comma-separated list to permit users to authenticate against multiple fields. For example, if you specify uid,mailid , a user can be authenticated by providing either their user ID or their mail ID.
Base DN	The DN of the node where the search for a user would start. The base DN becomes the start location for loading users and groups. For performance reasons, ensure that the base DN is as specific as possible. For example, if all of your user accounts and groups are on the directory server in the Users folder, and your domain name is extremenetworks.com , the base DN value would be cn=Users,dc=extremenetworks,dc=com .

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration > User Management** and click the **Authentication** icon.
- 3 From the **Authentication Module** list box, select **LDAP**.
- 4 Click **Add** and complete the basic configuration parameters.
- 5 Under **Connection Settings**, select the type of bind connection.
- 6 If you are using an authenticated bind, provide the authentication information.
For example, if the login name is admin and the domain is **extremenetworks.com**, the **Login DN** would be **cn=admin,dc=extremenetworks,dc=com**.
- 7 Click **Test connection** to test the connection information.
You must have a successful connection to the LDAP server before you can continue with the remaining steps.
- 8 Select the authorization method to use.
 - If you want the LDAP server to verify only the user name and password information, choose **Local**. No authorization information is exchanged between the LDAP server and the Extreme Security console.
 - If you want to specify which attributes can be used to determine authorization levels, choose **User attributes**.
 - If you want users to inherit role-based access permissions after they authenticate with the LDAP server, choose **Group**.
- 9 If you are using **Group** authorization, specify the accept and deny privilege groups.
 - a In the **Group Member Field**, provide the LDAP attribute that is used to define the users group membership.
 - b Click the plus (+) or minus (-) icon to add or remove privilege groups.
The user role privilege options control which Extreme Security components the user has access to. The security profile privilege options control the Extreme Security data that each user has access to.
- 10 Click **Save**.
- 11 Click **Manage synchronization** to exchange authentication and authorization information between the LDAP server and the Extreme Security console.
 - a If you are configuring the LDAP connection for the first time, click **Run Synchronization Now** to synchronize the data.

- b Specify the frequency for automatic synchronization.
 - c Click **Close**.
- 12 Repeat the steps to add more LDAP servers, and click **Save** when complete.

Multiple LDAP repositories

You can configure Extreme Networks Security Analytics to map entries from multiple LDAP repositories into a single virtual repository.

If multiple repositories are configured, users must specify the domain name when they log in to indicate which repository is to use for authentication.

For example, a Extreme Security system has two LDAP repositories configured. Repository_1 is configured to use domain `extremenetworks.com` and Repository_2 is configured to use domain `extremenetworks.ca`. When a user tries to log in, they must specify the domain name in the user name field, such as `extremenetworks.com\username`.

User information is automatically imported from the LDAP server for repositories that use user attributes or group authorization. For repositories that use local authorization, you must create users directly on the Extreme Security system.

Example: least privileged access configuration and set up

Grant users only the minimum amount of access that they require to do their day-to-day tasks.

You can assign different privileges for Extreme Security data and Extreme Security capabilities. You can do this assignment by specifying different accept and deny groups for security profiles and user roles. Accept groups assign privileges and deny groups restrict privileges.

Let's look at an example. Your company hired a group of student interns. John is in his final year of a specialized cyber security program at the local university. He was asked to monitor and review known network vulnerabilities and prepare a remediation plan based on the findings. Information about the company's network vulnerabilities is confidential.

As the Extreme Security administrator, you must ensure that the student interns have limited access to data and systems. Most student interns must be denied access to Extreme Security Vulnerability Manager, but John's special assignment requires that he has this access. Your organization's policy is that student interns never have access to the Extreme Security API.

The following table shows that John must be a member of the `company.interns` and `qvm.interns` groups to have access to Risk Manager and Extreme Security Vulnerability Manager.

Table 8: User role privilege groups

User Role	Accept	Deny
Admin	qradar.admin	company.firedemployees
QVM	qradar.qvm qvm.interns	company.firedemployees qradar.qrm company.interns
QRM	qradar.qrm company.interns	company.firedemployees

The following table shows that the security profile for *qvm.interns* restricts John from accessing the Extreme Security API.

Table 9: Security profile privilege groups

Security profile	Accept	Deny
QVM	qradar.secprofile.qvm	company.firedemployees
API	qradar.secprofile.qvm.api	company.firedemployees qradar.secprofile.qvm.interns

Displaying hover text for LDAP information

You create an LDAP properties configuration file to display LDAP user information as hover text. This configuration file queries the LDAP database for LDAP user information that is associated with events or assets (if available).

The web server must be restarted after the LDAP properties is created. Consider scheduling this task during a maintenance window when no active users are logged in to the system.

The following example lists properties that you can add to an `ldap.properties` configuration file.

```
ldap.url=ldap://LDAPserver.example.com:389
ldap.authentication=simple
ldap.userName=user.name
ldap.password=your.encrypted.password
ldap.basedn=O=IBM,C=US ldap.filterString=(amp(objectclass=user)(samaccountname=
%USER%))
ldap.attributes.displayName=Name
ldap.attributes.email=Email
ldap.attributes.employeeID=EmployeeID
ldap.attributes.department=Department
```

- 1 Use SSH to log in to Extreme Networks Security Analytics as a root user.
- 2 To encrypt the LDAP user password, run the `/opt/qradar/bin/runjava.sh com.qllabs.core.util.PasswordEncrypt [password]` script.
- 3 Use a text editor to create the `/opt/qradar/conf/ldap.properties` configuration file.

- 4 Specify the location and authentication information to access the remote LDAP server.
 - a Specify the URL of the LDAP server and the port number.
Use `ldaps://` or `ldap://` to connect to the remote server, for example, `ldap.url=ldaps://LDAPserver.example.com:389`.
 - b Type the authentication method that is used to access the LDAP server.
Administrators can use the simple authentication method, for example, `ldap.authentication=simple`.
 - c Type the user name that has permissions to access the LDAP server, for example, `ldap.userName=user.name`.
 - d To authenticate to the remote LDAP server, type the encrypted LDAP user password for the user, for example, `ldap.password=password`.
 - e Type the base DN used to search the LDAP server for users, for example, `ldap.basedn=BaseDN`.
 - f Type a value to use for the search parameter filter in LDAP.
For example, in Extreme Networks Security Analytics, when you hover over `ldap.filterString=(&(objectclass=user)(samaccountname=%USER%))`, the `%USER%` value is replaced by the user name.
- 5 Type one or more attributes to display in the hover text.
You must include at least one LDAP attribute. Each value must use this format:
`ldap.attributes.AttributeName=Descriptive text to show in UI.`
- 6 Verify that there is read-level permission for the `ldap.properties` configuration file.
- 7 Log in to Extreme Security as an administrator.
- 8 On the **Admin** tab, select **Advanced > Restart Web Server**.

Administrators can hover over the **Username** field on the **Log Activity** tab, or hover over the **Last User** field on the **Assets** tab (if available) to display more information about the LDAP user.

Configuring SSL or TLS certificates

If you use an LDAP directory server for user authentication and you want to enable SSL encryption or TLS authentication, you must configure your SSL or TLS certificate.

- 1 Using SSH, log in to your system as the root user.
 - a User name: `root`
 - b Password: `<password>`
- 2 Type the following command to create the `/opt/qradar/conf/trusted_certificates/` directory:


```
mkdir -p /opt/qradar/conf/trusted_certificates
```
- 3 Copy the SSL or TLS certificate from the LDAP server to the `/opt/qradar/conf/trusted_certificates` directory on your system.
- 4 Verify that the certificate file name extension is `.cert`, which indicates that the certificate is trusted.
The QRadar system only loads `.cert` files.

User role access and permissions


Use the **User Role Management** window parameters to restrict access to Extreme Networks Security Analytics capabilities.

The following table describes the **User Role Management** window parameters. The parameters that are visible on the **User Role Management** window are dependent on which Extreme Security components are installed.

Table 10: Description of User Role Management window parameters

Parameter	Description								
User Role name	A unique name for the role.								
Admin	Grants administrative access to the user interface. You can grant specific Admin permissions: <table> <tr> <td>Administrator Manager</td><td>Grants administrative access to the user interface. You grant specific Admin permissions.</td></tr> <tr> <td>Remote Networks and Services Configuration</td><td>Grants permission to configure remote networks and services on the Admin tab.</td></tr> <tr> <td>System Administrator</td><td>Grants permission to access all areas of the user interface. Users who have this access cannot edit other administrator accounts.</td></tr> </table>	Administrator Manager	Grants administrative access to the user interface. You grant specific Admin permissions.	Remote Networks and Services Configuration	Grants permission to configure remote networks and services on the Admin tab.	System Administrator	Grants permission to access all areas of the user interface. Users who have this access cannot edit other administrator accounts.		
Administrator Manager	Grants administrative access to the user interface. You grant specific Admin permissions.								
Remote Networks and Services Configuration	Grants permission to configure remote networks and services on the Admin tab.								
System Administrator	Grants permission to access all areas of the user interface. Users who have this access cannot edit other administrator accounts.								
Offenses	Grants the access to all the functions on the Offenses tab. You can grant specific permissions: <table> <tr> <td>Assign Offenses to Users</td><td>Grants permission to assign offenses to other users.</td></tr> <tr> <td>Maintain Custom Rules</td><td>Grants permission to create and edit custom rules.</td></tr> <tr> <td>Manage Offense Closing Reasons</td><td>Grants permission to manage offense closing reasons.</td></tr> <tr> <td>View Custom Rules</td><td>Grants permission to view custom rules. If granted to a user role that does not also have the Maintain Custom Rules permission, the user role cannot create or edit custom rules.</td></tr> </table>	Assign Offenses to Users	Grants permission to assign offenses to other users.	Maintain Custom Rules	Grants permission to create and edit custom rules.	Manage Offense Closing Reasons	Grants permission to manage offense closing reasons.	View Custom Rules	Grants permission to view custom rules. If granted to a user role that does not also have the Maintain Custom Rules permission, the user role cannot create or edit custom rules.
Assign Offenses to Users	Grants permission to assign offenses to other users.								
Maintain Custom Rules	Grants permission to create and edit custom rules.								
Manage Offense Closing Reasons	Grants permission to manage offense closing reasons.								
View Custom Rules	Grants permission to view custom rules. If granted to a user role that does not also have the Maintain Custom Rules permission, the user role cannot create or edit custom rules.								
Log Activity	Grants access to functions in the Log Activity tab. You can also grant specific permissions: <table> <tr> <td>Maintain Custom Rules</td><td>Grants permission to create or edit rules that are displayed on the Log Activity tab.</td></tr> <tr> <td>Manage Time Series</td><td>Grants permission to configure and view time series data charts.</td></tr> <tr> <td>User Defined Event Properties</td><td>Grants permission to create custom event properties. For more information about custom event properties, see the <i>Users Guide</i> for your product.</td></tr> <tr> <td>View Custom Rules</td><td>Grants permission to view custom rules. If granted to a user role that does not also have the Maintain Custom Rules permission, the user role cannot create or edit custom rules.</td></tr> </table>	Maintain Custom Rules	Grants permission to create or edit rules that are displayed on the Log Activity tab.	Manage Time Series	Grants permission to configure and view time series data charts.	User Defined Event Properties	Grants permission to create custom event properties. For more information about custom event properties, see the <i>Users Guide</i> for your product.	View Custom Rules	Grants permission to view custom rules. If granted to a user role that does not also have the Maintain Custom Rules permission, the user role cannot create or edit custom rules.
Maintain Custom Rules	Grants permission to create or edit rules that are displayed on the Log Activity tab.								
Manage Time Series	Grants permission to configure and view time series data charts.								
User Defined Event Properties	Grants permission to create custom event properties. For more information about custom event properties, see the <i>Users Guide</i> for your product.								
View Custom Rules	Grants permission to view custom rules. If granted to a user role that does not also have the Maintain Custom Rules permission, the user role cannot create or edit custom rules.								

Table 10: Description of User Role Management window parameters (continued)

Parameter	Description								
Assets	<div>  <p>Note This permission is displayed only if Extreme Networks Security Vulnerability Manager is installed on your system.</p> </div> <p>Grants access to the function in the Assets tab. You can grant specific permissions:</p> <table> <tr> <td>Perform VA Scans</td><td>Grants permission to complete vulnerability assessment scans. For more information about vulnerability assessment, see the <i>Managing Vulnerability Assessment guide</i>.</td></tr> <tr> <td>Remove Vulnerabilities</td><td>Grants permission to remove vulnerabilities from assets.</td></tr> <tr> <td>Server Discovery</td><td>Grants permission to discover servers.</td></tr> <tr> <td>View VA Data</td><td>Grants permission to vulnerability assessment data. For more information about vulnerability assessment, see the <i>Managing Vulnerability Assessment guide</i>.</td></tr> </table>	Perform VA Scans	Grants permission to complete vulnerability assessment scans. For more information about vulnerability assessment, see the <i>Managing Vulnerability Assessment guide</i> .	Remove Vulnerabilities	Grants permission to remove vulnerabilities from assets.	Server Discovery	Grants permission to discover servers.	View VA Data	Grants permission to vulnerability assessment data. For more information about vulnerability assessment, see the <i>Managing Vulnerability Assessment guide</i> .
Perform VA Scans	Grants permission to complete vulnerability assessment scans. For more information about vulnerability assessment, see the <i>Managing Vulnerability Assessment guide</i> .								
Remove Vulnerabilities	Grants permission to remove vulnerabilities from assets.								
Server Discovery	Grants permission to discover servers.								
View VA Data	Grants permission to vulnerability assessment data. For more information about vulnerability assessment, see the <i>Managing Vulnerability Assessment guide</i> .								
Network Activity	<p>Grants access to all the functions in the Network Activity tab. You can grant specific access to the following permissions:</p> <table> <tr> <td>Maintain Custom Rules</td><td>Grants permission to create or edit rules that are displayed on the Network Activity tab.</td></tr> <tr> <td>Manage Time Series</td><td>Grants permission to configure and view time series data charts.</td></tr> <tr> <td>View Custom Rules</td><td>Grants permission to view custom rules. If the user role does not also have the Maintain Custom Rules permission, the user role cannot create or edit custom rules.</td></tr> </table>	Maintain Custom Rules	Grants permission to create or edit rules that are displayed on the Network Activity tab.	Manage Time Series	Grants permission to configure and view time series data charts.	View Custom Rules	Grants permission to view custom rules. If the user role does not also have the Maintain Custom Rules permission, the user role cannot create or edit custom rules.		
Maintain Custom Rules	Grants permission to create or edit rules that are displayed on the Network Activity tab.								
Manage Time Series	Grants permission to configure and view time series data charts.								
View Custom Rules	Grants permission to view custom rules. If the user role does not also have the Maintain Custom Rules permission, the user role cannot create or edit custom rules.								
Reports	<p>Grants permission to access to all the functions in the Reports tab. You can grant users-specific permissions:</p> <table> <tr> <td>Distribute Reports via Email</td><td>Grants permission to distribute reports through email.</td></tr> <tr> <td>Maintain Templates</td><td>Grants permission to edit report templates.</td></tr> </table>	Distribute Reports via Email	Grants permission to distribute reports through email.	Maintain Templates	Grants permission to edit report templates.				
Distribute Reports via Email	Grants permission to distribute reports through email.								
Maintain Templates	Grants permission to edit report templates.								
Vulnerability Manager	<p>Grants permission to Extreme Security Vulnerability Manager function. Extreme Networks Security Vulnerability Manager must be activated. For more information, see the <i>Extreme Networks Security Vulnerability Manager User Guide</i>.</p>								
Forensics	<p>Grants permission to Extreme Security Incident Forensics capabilities.</p> <table> <tr> <td>Create cases in Incident Forensics</td><td>Grants permission to create cases for collections of imported document and pcap files.</td></tr> </table>	Create cases in Incident Forensics	Grants permission to create cases for collections of imported document and pcap files.						
Create cases in Incident Forensics	Grants permission to create cases for collections of imported document and pcap files.								
IP Right Click Menu Extensions	Grants permission to options added to the right-click menu.								
Platform Configuration	<p>Grants permission to Platform Configuration services.</p> <table> <tr> <td>Dismiss System Notifications</td><td>Grants permission to hide system notifications from the Messages tab.</td></tr> <tr> <td>View System Notifications</td><td>Grants permission to view system notifications from the Messages tab.</td></tr> </table>	Dismiss System Notifications	Grants permission to hide system notifications from the Messages tab.	View System Notifications	Grants permission to view system notifications from the Messages tab.				
Dismiss System Notifications	Grants permission to hide system notifications from the Messages tab.								
View System Notifications	Grants permission to view system notifications from the Messages tab.								

Security profile parameters

The following table provides descriptions of the **Security Profile Management** window parameters:

Table 11: Security Profile Management window parameters

Parameter	Description
Security Profile Name	Type a unique name for the security profile. The security profile name must meet the following requirements: <ul style="list-style-type: none"> • Minimum of 3 characters • Maximum of 30 characters
Description	Optional. Type a description of the security profile. The maximum number of characters is 255.

User Management window parameters

The following table provides descriptions of User Management window parameters:

Table 12: User Management window parameters

Parameter	Description
Username	Displays the user name of this user account.
Description	Displays the description of the user account.
E-mail	Displays the email address of this user account.
User Role	Displays the user role that is assigned to this user account. User Roles define what actions the user has permission to perform.
Security Profile	Displays the security profile that is assigned to this user account. Security Profiles define what data the user has permission to access.

User management window toolbar

User management window toolbar functions

The following table provides descriptions of the **User Management** window toolbar functions:

Table 13: User Management window toolbar functions

Function	Description
New	Click this icon to create a user account. For more information about how to create a user account, see Creating a user account on page 23.
Edit	Click this icon to edit the selected user account.
Delete	Click this icon to delete the selected user account.
Search Users	In this text box, you can type a keyword and then press Enter to locate a specific user account.

User Details window parameters

User Details window parameters

The following table provides descriptions of the **User Details** window parameters:

Table 14: User Details window parameters

Parameter	Description
Username	Type a unique user name for the new user. The user name must contain a maximum of 30 characters.
E-mail	Type the user's email address. The email address must meet the following requirements: <ul style="list-style-type: none"> • Must be a valid email address • Minimum of 10 characters • Maximum of 255 characters
Password	Type a password for the user to gain access. The password must meet the following criteria: <ul style="list-style-type: none"> • Minimum of 5 characters • Maximum of 255 characters
Confirm Password	Type the password again for confirmation.
Description	Optional. Type a description for the user account. The maximum number of characters is 2,048.
User Role	From the list box, select the user role that you want to assign to this user. To add, edit, or delete user roles, you can click the Manage User Roles link. For information on user roles, see Role management on page 18.
Security Profile	From the list box, select the security profile that you want to assign to this user. To add, edit, or delete security profiles, you can click the Manage Security Profiles link. For information on security profiles, see Managing security profiles on page 20.

4 System and licenses management

System and License Management window overview

License management checklist

System management

Access setting management

Time server configuration

You can manage the licenses, high availability (HA), and systems in your deployment.

You must allocate a license for each system in your deployment, including software appliances. Extreme Security Event Collectors do not require a license.

When you install a Extreme Security system, a default license key provides you with access to the user interface for five weeks. Before the default license expires, you must allocate a license key to your system. You can also add licenses to enable Extreme Security products, such as Extreme Security Vulnerability Manager.

There is a 14-day grace period to reallocate a license. You can unlock a license if the key is uploaded, after a host is patched with a fix, or after an unlock key is uploaded. After the grace period is passed, the license is locked to the system.

If your license status is **Invalid**, the license must be replaced. The status might indicate that your license was altered without authorization.

A license remains undeployed until you deploy the license change.

System and License Management window overview

You can use the **System and License Management** window to manage your license keys, restart or shut down your system, and configure access settings.

The toolbar on the **System and License Management** window provides the following functions:

Table 15: System and License Management toolbar functions

Function	Description
Allocate License to System	Use this function to allocate a license to a system. When you select Licenses from the Display list box, the label on this function changes to Allocate System to Licenses .
Upload License	Use this function to upload a license to your Console. For more information, see Uploading a license key on page 41.

Table 15: System and License Management toolbar functions (continued)

Function	Description
Actions (License)	<p>If you select Licenses from the Display list box in the Deployment Details pane, the following functions are available on the Actions menu:</p> <p>If you select Revert Allocation on a deployed license within the allocation grace period, which is 14 days after deployment, the license state changes to Unlocked so that you can reallocate the license to another system.</p>
Actions (System)	<p>If you select Systems from the Display list box in the Deployment Details pane, the following functions are available on the Actions menu:</p> <ul style="list-style-type: none"> • View System - Select a system, and then select this option to view the System Details window. For more information, see Viewing system details on page 43. • Add HA Host - Select a system, and then select this option to add an HA host to the system to form an HA cluster. For more information about HA, see the <i>High Availability Guide</i> for your product. • Revert Allocation - Select this option to undo staged license changes. The configuration reverts to the last deployed license allocation. <p>If you select Revert Allocation on a deployed license within the allocation grace period, which is 14 days after deployment, the license state changes to Unlocked so that you can reallocate the license to another system.</p> <ul style="list-style-type: none"> • Manage System - Select a system, and then select this option to open the System Setup window, which you can use to configure firewall rules, interface roles, passwords, and system time. For more information, see Access setting management on page 47. • Restart Web Server - Select this option to restart the user interface, when required. For example, you might be required to restart your user interface after you install a new protocol that introduces new user interface components. • Shutdown System - Select a system, and then select this option to shut down the system. For more information, see Shutting down a system on page 45. • Restart System - Select a system, and then select this option to restart the system. For more information, see Restarting a system on page 45.

When you select **Licenses** from the **Display** list box in the Deployment Details pane, the **System and License Management** window displays the following information:

Table 16: System and License Management window parameters - Licenses view

Parameter	Description
Host Name	Displays the host name of the system that is allocated to this license.
Host IP	Displays the IP address of the system that is allocated to this license.
Appliance Type	Displays the appliance type of the system that is allocated to this license.
License Identity	Displays the name of the Extreme Networks Security Analytics product this license provides.

Table 16: System and License Management window parameters - Licenses view (continued)

Parameter	Description
License Status	Displays the status of the license that is allocated to this system. Statuses include: <ul style="list-style-type: none"> • Unallocated - Indicates that this license is not allocated to a system. • Undeployed - Indicates that this license is allocated to a system, but you have not deployed the allocation change. This means that the license is not active in your deployment yet. • Deployed - Indicates that this license is allocated and active in your deployment. • Unlocked - Indicates that this license has been unlocked. You can unlock a license if it was deployed within the last 10 days. This is the default grace period to reallocate a license. After the grace period is passed, the license is locked to the system. If you must unlock a license after that period, contact Customer Support. • Invalid - Indicates that this license is not valid and must be replaced. This status might indicate that your license was altered without authorization.
License Expiration Date	Displays the expiration date of this license.
Event Rate Limit	Displays the event rate limit that your license allows.

License management checklist

You use the options available on the **System and License Management** window to manage your license keys.

A default license key provides you with access to the user interface for five weeks. You must allocate a license key to your system.

You must set up the Extreme Security system before users can use the tools. Begin by obtaining a license key. After you have a license key, you must upload it to the console and allocate it to a system.

During the initial set up of a system you must complete the following tasks:

- 1 Obtain a license key by one of the following methods:
 - For a new or updated license key, contact your local sales representative.
 - For all other technical issues, contact Customer Support.
- 2 Upload your license key.

When you upload a license key, it is listed in the **System and License Management** window, but remains unallocated. For more information, see [Uploading a license key](#) on page 41
- 3 Allocate your license to a system or allocate a system to a license.
- 4 To deploy your changes, from the **Admin** tab menu, click **Advanced > Deploy Full Configuration**.

When you deploy the full configuration, Extreme Security restarts all services. Data collection for events stops until the deployment completes.

Uploading a license key

You must upload a license key to the Console when you install a new Extreme Security system, update an expired license, or add a Extreme Security product, such as Extreme Security Vulnerability Manager, to your deployment.

Choose one of the following options for assistance with your license key:

- 1 For a new or updated license key, contact your local sales representative.
- 2 For all other technical issues, contact Customer Support.

If you log in to the user interface and your Console license key expired, you are automatically directed to the **System and License Management** window. You must upload a license key before you can continue. If one of your non-Console systems includes an expired license key, a message is displayed when you log in indicating a system requires a new license key. You must access the **System and License Management** window to update that license key.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration**.
- 3 Click the **System and License Management** icon.
- 4 On the toolbar, click **Upload License**.
- 5 In the dialog box, click **Select File**.
- 6 On the **File Upload** window, locate and select the license key.
- 7 Click **Open**.
- 8 Click **Upload**.

The license is uploaded to your Console and is displayed in the **System and License Management** window. By default, the license is not allocated.

[Allocating a system to a license](#) on page 45

Allocating a license to a system

Use the options in the **System and License Management** window to allocate a license.

When you install a Extreme Security system, a default license key provides you with access to the user interface for five weeks. Before the default license expires, you must allocate a license key to your system. You can also add licenses to enable Extreme Security products, such as Vulnerability Manager.

You can allocate multiple licenses to a system. For example, in addition to Extreme Networks Security Log Manager, you can allocate Extreme Networks Security Risk Manager, and Extreme Networks Security Vulnerability Manager to your Extreme Security Console system.

License Status displays the status of the license that is allocated to this system. Statuses include:

- **Unallocated** - Indicates that this license is not allocated to a system.
- **Undeployed** - Indicates that this license is allocated to a system, but you have not deployed the allocation change. This means that the license is not active in your deployment yet.
- **Deployed** - Indicates that this license is allocated and active in your deployment.
- **Unlocked** - Indicates that this license has been unlocked. You can unlock a license if it has been deployed within the last 14 days. This is the default grace period to reallocate a license. After the

grace period is passed, the license is locked to the system. If you must unlock a license after that period, contact Customer Support.

- **Invalid** - Indicates that this license is not valid and must be replaced. This status may indicate that your license has been altered without authorization.
- 1 Click the **Admin** tab.
 - 2 On the navigation menu, click **System Configuration**.
 - 3 Click the **System and License Management** icon.
 - 4 From the **Display** list box, select **Licenses**.
 - 5 Select an unallocated license.
 - 6 Click **Allocate System to License**.
 - 7 Optional: To filter the list of licenses, type a keyword in the **Upload License** search box.
 - 8 From the list of licenses, select a license.
 - 9 Select a system.
 - 10 Click **Allocate License to System**.

Reverting an allocation

You can revert an allocated license within the 14 day grace period.

After you allocate a license to a system and before you deploy your configuration changes, you can undo the license allocation. When you undo the license allocation, the license that was last allocated and deployed on the system is maintained.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration**.
- 3 Click the **System and License Management** icon.
- 4 From the **Display** list box, select **Licenses**.
- 5 Select the license that you want to revert.
- 6 Click **Actions > Revert Allocation**.

Viewing license details

A license key provides information and enforces the limits and abilities on an Extreme Networks Security Analytics system.

From the **System and License Management** window, you can view license details, such as the number of allowable log sources and the expiration dates.



Note

If you exceed the limit of configured logs sources, an error message is displayed. If log sources are auto-discovered and your limit is exceeded, they are automatically disabled. To extend the number of log sources, contact your sales representative.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration**.
- 3 Click the **System and License Management** icon.

- 4 From the **Display** list box, select **Licenses**.
- 5 To display the **Current License Details** window for a license, double-click the license that you want to view.

From the **Current License** window, you can complete the following tasks:

- Click **Upload Licenses** to upload a license. See [Uploading a license key](#).
- Click **Allocate License to System** on the toolbar to assign a license. See [Allocating a license to a system](#).

Exporting a license

Export license key information to a desktop system.

You can export license key information to an external file on your desktop system.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration**.
- 3 Click the **System and License Management** icon.
- 4 From the **Display** list box, select **Licenses**.
- 5 From the **Actions** menu, select **Export Licenses**.
- 6 Select one of the following options:
 - **Open with** - Opens the license key data using the selected application.
 - **Save File** - Saves the file to your desktop.
- 7 Click **OK**.

System management

Use the **System and License Management** window to manage systems in your deployment.

You use the options available on the **System and License Management** window to manage the systems in your deployment. You can view system details, assign a license to a system, or restart and shut down a system.

Viewing system details

View information about the system, including licenses from the **System Details** window.

Open the **System Details** window to view information about the system and the list of licenses that are allocated to the system.

The license list provides the following details for each license that is allocated to this system:

Table 17: License parameters

Parameter	Description
License Identity	Displays the name of the Extreme Security product this license provides.
License Status	Displays the status of the license that is allocated to this system. Statuses include: <ul style="list-style-type: none"> • Unallocated - Indicates that this license is not allocated to a system. • Undeployed - Indicates that this license is allocated to a system, but you have not deployed the allocation change. This means that the license is not active in your deployment yet. • Deployed - Indicates that this license is allocated and active in your deployment. • Unlocked - Indicates that this license has been unlocked. You can unlock a license if it has been deployed within the last 10 days. This is the default grace period to reallocate a license. After the grace period is passed, the license is locked to the system. If you need to unlock a license after that period, contact Customer Support. • Invalid - Indicates that this license is not valid and must be replaced. This status may indicate that your license has been altered without authorization.
License Appliance Types	Displays the appliance type that this license is valid for.
License Expiration Date	Displays the expiration date of this license.
Event Rate Limit	Displays the event rate limit this license allows.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration**.
- 3 Click the **System and License Management** icon.
- 4 From the **Display** list box, select **Systems**.
- 5 To display the system details, double-click the system that you want to view.

From the **system details** window, you can complete the following tasks:

- Select a license and click **View License**. See [Viewing license details](#) on page 42.
- Click **Upload Licenses** to upload a license. See [Uploading a license key](#) on page 41.
- Click **Allocate License to System** on the toolbar to assign a license. See [Allocating a license to a system](#).

System health

The System health view shows system notifications and health information for the Extreme Networks Security Analytics host.

Select **Admin > System Configuration > System Health** icon in the System Configuration area on the Admin tab to view CPU usage, network reads and writes, disk reads and writes, memory usage, and events per second (EPS).

Hover over a graph to view more information, and the metric being graphed.

Allocating a system to a license

After you obtain and upload a license, use the options in the **System and License Management** window to allocate a license.

You can allocate multiple licenses to a system. For example, in addition to Extreme Networks Security Log Manager, you can allocate Extreme Networks Security Risk Manager, and Extreme Networks Security Vulnerability Manager to your Extreme Security Console system.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration**.
- 3 Click the **System and License Management** icon.
- 4 From the **Display** list box, select **Systems**.
- 5 Select an available system.
- 6 Click **Allocate License to System**.
- 7 To filter the list of licenses, type a keyword in the Upload License search box.
- 8 From the list of licenses, select a license.
- 9 Select a system.
- 10 Click **Allocate License to System**.

Restarting a system

Use the **Restart System** option on the **System and License Management** window to restart a system in your deployment.

Data collection stops while the system is shutting down and restarting.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration**.
- 3 Click the **System and License Management** icon.
- 4 From the **Display** list box, select **Systems**.
- 5 Select the system that you want to restart.
- 6 From the **Actions** menu, select **Restart System**.

Shutting down a system

Use the **Shutdown** option on the **System and License Management** window to shut down a system.

Data collection stops while the system is shutting down.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration**.
- 3 Click the **System and License Management** icon.
- 4 From the **Display** list box, select **Systems**.
- 5 Select the system that you want to shut down.
- 6 From the **Actions** menu, select **Shutdown**.

Exporting system details

Use the **Export Systems** option on the **System and License Management** window to export system information to an external file on your desktop system

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration**.
- 3 Click the **System and License Management** icon.
- 4 From the **Display** list box, select **Systems**.
- 5 From the **Actions** menu, select **Export Systems**.
- 6 Select one of the following options:
 - **Open with** - Opens the license key data by using the selected application.
 - **Save File** - Saves the file to your desktop.
- 7 Click **OK**.

Collecting log files

Extreme Security log files contain detailed information about your deployment, such as host names, IP addresses, and email addresses. If you need help with troubleshooting, you can collect the log files and send them to Extreme Networks® Customer Support.

You can collect log files directly from the Extreme Security.

You can collect the log files for one or more host systems at the same time. The time that is required to collect the log files depends on the size of your deployment and the number of hosts that you want to include in the log file collection. The Extreme Security console log files are automatically included in each log file collection.

You can continue to use the Extreme Security console while the log file collection is running. If the system is actively collecting log files, you cannot initiate a new collection request. You must cancel the active collection process and start another collection.

When the log file collection process completes, a system notification appears on the **System Monitoring** dashboard.

- 1 Click the **Admin** tab.
- 2 On the navigation window, click **System Configuration** and click the **System and License Management** icon.
- 3 Press Ctrl and click each host that you want to include in the log file collection.
- 4 Click **Actions > Collect Log Files**.
- 5 Click **Advanced Options** and choose the options for the log file collection.

Encrypted log file collections can be decrypted only by Extreme Networks® Customer Support. If you want access to the log file collection, do not encrypt the file.
- 6 Click **Collect Log Files**.
- 7 Under **System Support Activities Messages**, a message indicates the status of the collection process. To cancel an active log file collection process, click the **X** in the notification message.
- 8 To download the log file collection, click **Click here to download files** in the **Log file collection completed successfully** notification.

Deploying managed hosts and components after installation

After installation, you can add managed hosts to your deployment. To help distribute processing, you can add Extreme Security Event Collectors, or other appliances in your deployment.

You can configure the components, such as vulnerability scanners, on a managed host.



Note

Use the **Deployment editor** to add and configure components of your software install. You can't see visualizations of your deployment in **Deployment actions**.

If you configured Extreme Networks Security Vulnerability Manager in your deployment, you can add vulnerability scanners and a vulnerability processor. For more information, see the *Extreme Networks Security Vulnerability Manager User Guide*.

If you configured Extreme Networks Security Risk Manager in your deployment, you can add a managed host. For more information, see *Extreme Networks Security Risk Manager Installation Guide*.

- 1 Click the **Admin** tab.
- 2 In the **System Configuration** pane, click **System and License Management**.
- 3 From the host table, select one of the following that you want to manage.
 - Extreme Security Console
 - Extreme Security managed host
- 4 From the **Deployment actions** menu, choose an action.
- 5 Enter the information for the action that you want to do.
- 6 Close the **System and License Management** window.
- 7 Click the **Admin** tab.
- 8 On the **Admin** tab menu, click **Deploy Changes**.

Related Links

[Adding components](#) on page 116

Access setting management

You can use the **System Setup** window to configure firewall rules, interface roles, passwords, and system time.

If you require network configuration changes, such as an IP address change, to your Console and non-Console systems after your deployment is initially installed, you must use the **qchange_netsetup** utility to make these changes. For more information about network settings, see the *Installation Guide* for your product.

Configuring firewall access

You can configure local firewall access to enable communications between devices and Extreme Networks Security Analytics. Also, you can define access to the **System Setup** window.

Only the listed managed hosts that are listed in the **Device Access** box have access to the selected system. For example, if you enter one IP address, only that IP address is granted access to the Console. All other managed hosts are blocked.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration**.
- 3 Click the **System and License Management** icon.
- 4 From the **Display** list box, select **Systems**.
- 5 Select the host for which you want to configure firewall access settings.
- 6 From the **Actions** menu, select **Manage System**.
- 7 Log in to the **System Setup** window. The default is:
 - a **User Name:** `root`
 - b **Password:** `<password>`

The user name and password are case sensitive.
- 8 From the menu, select **Managed Host Config > Local Firewall**.
- 9 Configure the following Device Access parameters:

Option	Description
Device Access	In the Device Access box, include any Extreme systems that you want to access to this managed host. Only the listed managed hosts have access. For example, if you enter one IP address, only that IP address is granted access to the managed host. All other managed hosts are blocked.
IP Address	Type the IP address of the managed host you want to have access.
Protocol	Select the protocol that you want to enable access for the specified IP address and port. Options include: <ul style="list-style-type: none"> • UDP - Allows UDP traffic. • TCP - Allows TCP traffic. • Any - Allows any traffic.
Port	Type the port on which you want to enable communications.

- 10 Click **Allow**.
- 11 Configure the System Administration Web Control parameter:

Type the IP addresses of managed hosts that you want to allow access to the System Setup window in the **IP Address** field. Only listed IP addresses have access to the user interface. If you leave the field blank, all IP addresses have access.

Make sure that you include the IP address of your client desktop you want to use to access the user interface. Failing to do so might affect connectivity.
- 12 Click **Allow**.
- 13 Click **Apply Access Control**.
- 14 Wait for the **System Setup** window to refresh before you continue to another task.

Updating your host setup

You can use the **System Setup** window to configure the mail server you want to use and the global password for all systems in your Extreme Security deployment.

The global configuration password does not accept special characters. The global configuration password must be the same throughout your deployment. If you edit this password, you must also edit the global configuration password on all systems in your deployment.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration**.
- 3 Click the **System and License Management** icon.
- 4 From the **Display** list box, select **Systems**.
- 5 Select the host for which you want to update your host setup settings.
- 6 From the **Actions** menu, select **Manage System**.
- 7 Log in to the **System Setup** window. The default is:
 - a User Name: `root`
 - b Password: `<password>`

The user name and password are case-sensitive.
- 8 From the menu, select **Managed Host Config > QRadar Setup**.
- 9 In the **Mail Server** field, type the address for the mail server you want to use. Log Manager uses this mail server to distribute alerts and event messages. To use the mail server that Log Manager provides, type `localhost`.
- 10 In the **Enter the global configuration password**, type the password that you want to use to access the host. Type the password again for confirmation.
- 11 Click **Apply Configuration**.

Configuring interface roles

You can assign specific roles to the network interfaces on each managed host.

For assistance with determining the appropriate role for each interface, contact Customer Support.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration**.
- 3 Click the **System and License Management** icon.
- 4 From the **Display** list box, select **Systems**.
- 5 Select the host for which you want to configure interface role settings.
- 6 From the **Actions** menu, select **Manage System**.
- 7 Log in to the **System Setup** window. The default is:
 - a User Name: `root`
 - b Password: `<password>`

The user name and password are case-sensitive.
- 8 From the menu, select **Managed Host Config > Network Interfaces**.
- 9 For each listed network interface, select the role that you want to assign to the interface from the **Role** list box.
- 10 Click **Save Configuration**.
- 11 Wait for the **System Setup** window to refresh before you continue.

Changing the root password of your Extreme Security system

You can change the root password for your system.

When you change a password, make sure that you record the entered values. The root password does not accept the following special characters: apostrophe ('), dollar sign (\$), exclamation mark (!).

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration**.
- 3 Click the **System and License Management** icon.
- 4 From the **Display** list box, select **Systems**.
- 5 Select the host for which you want to configure interface role settings.
- 6 From the **Actions** menu, select **Manage System**.
- 7 Log in to the **System Setup** window. The default is:
 - a User Name: `root`
 - b Password: `<password>`

The user name and password are case-sensitive.

- 8 From the menu, select **Managed Host Config > Root Password**.
- 9 Update the password:
 - a **New Root Password** - Type the root password necessary to access the **System Setup** window.
 - b **Confirm New Root Password** - Type the password again for confirmation.
- 10 Click **Update Password**.

Time server configuration

You can configure your time server to use an RDATE server or you can manually configure your time server.

All system time changes must be made within the **System Time** page. You can change the system time on the host that operates the Console. The change is then distributed to all managed hosts in your deployment.

You are able to change the time for the following options:

- System time
- Hardware time
- Time Zone
- Time Server

Configuring your time server using RDATE

Use the Time server sync tab to configure your time server using RDATE.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration**.
- 3 Click the **System and License Management** icon.
- 4 From the **Display** list box, select **Systems**.

- 5 Select the host for which you want to configure system time settings.
- 6 From the **Actions** menu, select **Manage System**.
- 7 Log in to the **System Setup** window.
The user name and password are case-sensitive.
- 8 From the menu, select **Managed Host Config > System Time**.
- 9 Configure the time zone:
 - a Click the **Change time zone** tab.
 - b From the **Change timezone to** list box, select the time zone in which this managed host is located.
 - c Click **Save**.
- 10 Configure the time server:
 - a Click the **Time server sync** tab.
Configure the following parameters:

Table 18: Time server parameters

Parameter	Description
Timeserver hostnames or addresses	Type the time server host name or IP address.
Set hardware time too	Select this check box if you want to set the hardware time.
Synchronize on schedule?	Select one of the following options: <ul style="list-style-type: none"> • No - Select this option if you do not want to synchronize the time. Go to step c. • Yes - Select this option if you want to synchronize the time.
Simple Schedule	Select this option if you want the time update to occur at a specific time. After you select this option, select a simple schedule from the list box.
Times and dates are selected below	Select this option to specify time you want the time update to occur. After you select this option, select the times and dates in the list boxes.

- 11 Click **Sync and Apply**.

Manually configuring time settings for your system

Use the options on the **Set time** and **Change timezone** tabs to manually configure your time settings.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration**.
- 3 Click the **System and License Management** icon.
- 4 From the **Display** list box, select **Systems**.
- 5 Select the host for which you want to configure system time settings.
- 6 From the **Actions** menu, select **Manage System**.
- 7 Log in to the **System Setup** window. The default is:
 - a User Name: `root`
 - b Password: `<password>`

The user name and password are case-sensitive.

8 From the menu, select **Managed Host Config > System Time**.

9 Click the **Set time** tab.

The **Set Time** page is divided into tabs. You must save each setting before you continue. For example, when you configure system time, you must click **Apply** in the System Time pane before you continue.

10 Set the system time:

a Choose one of the following options:

- In the System Time pane, using the list boxes, select the current date and time you want to assign to the managed host.
- Click **Set system time to hardware time**.

b Click **Apply**.

11 Set the hardware time:

a Choose one of the following options:

- In the Hardware Time pane, using the list boxes, select the current date and time you want to assign to the managed host.
- Click **Set hardware time to system time**.

b Click **Save**.

12 Configure the time zone:

a Click the **Change time zone** tab.

b From the **Change Timezone To** list box, select the time zone in which this managed host is located.

c Click **Save**.

5 User information source configuration

User information source overview
Configuring the Tivoli Directory Integrator Server
Creating and managing user information source
Collecting user information

Configure your Extreme Networks Security Analytics system to collect user and group information from Identity and Access Management endpoints.

Extreme Networks Security Log Manager uses the information that is collected from the endpoints to enrich the user information that is associated with the traffic and events that occur on your network.

Extreme Networks Security Network Anomaly Detection uses the information that is collected from the endpoints to enrich the user information that is associated with the traffic and events that occur on your network.

User information source overview

You can configure a user information source to enable user information collection from an Identity and Access Management endpoint.

An Identity and Access Management endpoint is a product that collects and manages electronic user identities, group memberships, and access permissions. These endpoints are called user information sources.

Use the following utilities to configure and manage user information sources:

- **Tivoli Directory Integrator**- You must install and configure a Tivoli® Directory Integrator on a non-Extreme Security host.
- **UISConfigUtil.sh** - Use this utility to create, retrieve, update, or delete user information sources. You can use user information sources to integrate Log Manager using a Tivoli® Directory Integrator server.
- **GetUserInfo.sh** - Use this utility to collect user information from a user information source and store the information in a reference data collection. You can use this utility to collect user information on demand or on a schedule.

User information sources

A user information source is a configurable component that enables communication with an endpoint to retrieve user and group information.

Extreme Security systems support the following user information sources:

Table 19: Supported information sources

Information Source	Information that is collected
Microsoft Windows Active Directory (AD), version 2008 - Microsoft Windows AD is a directory service that authenticates and authorizes all users and computers that use your Windows network.	<ul style="list-style-type: none"> • full_name • user_name • user_principal_name • family_name • given_name • account_is_disabled • account_is_locked • password_is_expired • password_can_not_be_changed • no_password_expired • password_does_not_expire
Security Access Manager (ISAM), version 7.0 - ISAM is an authentication and authorization solution for corporate web, client/server, and existing applications. For more information, see your Security Access Manager (ISAM) documentation.	<ul style="list-style-type: none"> • name_in_rgy • first-name • last-name • account_valid • password_valid
Security Identity Manager (ISIM), version 6.0 - ISIM provides the software and services to deploy policy-based provisioning solutions. This product automates the process of provisioning employees, contractors, and Business Partners with access rights to the applications they need, whether in a closed enterprise environment or across a virtual or extended enterprise. For more information, see your Security Integration Manager (ISIM) documentation.	<ul style="list-style-type: none"> • Full name • DN

Reference data collections for user information

This topic provides information about how reference data collections store data collected from user information sources.

When Log Manager collects information from a user information source, it automatically creates a reference data collection to store the information. The name of the reference data collection is derived from the user information source group name. For example, a reference data collection that is collected from Microsoft™ Windows™ AD might be named Domain Admins.

The reference data collection type is a Map of Maps. In a Reference Map of Maps, data is stored in records that map one key to another key, which is then mapped to a single value.

For example:

- #
- # Domain Admins
- # key1,key2,data
- smith_j,Full Name,John Smith

- `smith_j,account_is_disabled,0`
- `smith_j,account_is_locked`
- `smith_j,password_does_not_expire,1`

For more information about reference data collections, see the *Reference Data Collections Technical Note*.

Integration workflow example

After user and group information is collected and stored in a reference data collection, there are many ways in which you can use the data in Extreme Networks Security Log Manager.

You can create meaningful reports and alerts that characterize user adherence to your company's security policies.

Consider the following example:

To ensure activities that are performed by privileged ISIM users comply with your security policies, you can complete the following tasks:

Create a log source to collect and parse audit data for each ISIM server from which the logs are collected. For more information about how to create a log source, see the *Extreme Networks Security Managing Log Sources Guide*.

- 1 Create a user information source for the ISIM server and collect ISIM Administrators user group information. This step creates a reference data collection that is called ISIM Administrators. See [Creating a user information source](#) on page 58.
- 2 Configure a building block to test for events in which the source IP address is the ISIM server and the user name is listed in the ISIM administrator reference data collection. For more information about building blocks, see the *User Guide* for your product.
- 3 Create an event search that uses the custom building block as a filter. For more information about event searches, see the *User Guide* for your product.
- 4 Create a custom report that uses the custom event search to generate daily reports on the audit activity of the privileged ISIM users. These generated reports indicate whether any ISIM administrator activity breaches your security policy. For more information about reports, see the *User Guide* for your product.



Note

If you want to collect application security logs, you must create a Device Support Module (DSM). For more information, see the *Extreme Networks Security DSM Configuration Guide*.

User information source configuration and management task overview

To initially integrate user information sources, you must perform the following tasks:

- 1 Configure a Tivoli® Directory Integrator server. See [Configuring the Tivoli Directory Integrator Server](#) on page 56.
- 2 Create and manage user information sources. See [Creating and managing user information source](#) on page 58.

- 3 Collect user information. See [Collecting user information](#) on page 61.

Configuring the Tivoli® Directory Integrator Server

For Extreme Networks Security Analytics to integrate with user information sources, you must install and configure a Tivoli® Directory Integrator on a non-Extreme Security host.

No configuration is required on your system; however, you must access your Console to obtain the `QRadarIAM_TDI.zip` file. Then, install and configure a Tivoli® Directory Integrator server on a separate host. If necessary, you must also create and import a self-signed certificate.

When you extract the `QRadarIAM_TDI.zip` file on the Tivoli® Directory Integrator server, the TDI directory is automatically created. The TDI directory includes the following files:

- `QradarIAM.sh`, which is the TDI start up script for Linux™
- `QradarIAM.bat`, which is the TDI start up script for Microsoft™ Windows™
- `QradarIAM.xml`, which is the TDI xml script and must be stored in the same location as the `QradarIAM.properties` file
- `QradarIAM.properties`, which is the properties file for TDI xml script

When you install Tivoli® Directory Integrator, you must configure a name for the Solutions directory. This task requires you to access the Solutions directory. Therefore, in the task steps, `<solution_directory>` refers to the name that you gave to the directory.

The following parameters are used to create and import certificates:

Table 20: Certification configuration parameters

Parameter	Description
<code><server_ip_address></code>	Defines the IP address of the Tivoli® Directory Integrator server.
<code><days_valid></code>	Defines the number of days that the certificate is valid.
<code><keystore_file></code>	Defines the name of the keystore file.
<code>-storepass <password></code>	Defines the password for keystore.
<code>- keypass <password></code>	Defines the password for the private/public key pair.
<code><alias></code>	Defines the alias for an exported certificate.
<code><certificate_file></code>	Defines the file name of the certificate.

- 1 Install Tivoli® Directory Integrator on a non-Extreme Security host. For more information on how to install and configure Tivoli® Directory Integrator, see your Tivoli® Directory Integrator (TDI) documentation.
- 2 Using SSH, log in to your Console as the root user.
 - a User name: `root`
 - b Password: `<password>`
- 3 Copy the `QRadarIAM_TDI.zip` file to the Tivoli® Directory Integrator server.
- 4 On the Tivoli® Directory Integrator server, extract the `QRadarIAM_TDI.zip` file in the Solutions directory.

- 5 Configure your Tivoli® Directory Integrator server to integrate with Extreme Security.
 - a Open the Tivoli® Directory Integrator `<solution_directory>/solution.properties` file.
 - b Uncomment the `com.ibm.di.server.autoload` property. If this property is already uncommented, note the value of the property.
 - c Choose one of the following options:
 - Change directories to the `autoload.tdi` directory, which contains the `com.ibm.di.server.autoload` property by default.
 - Create an `autoload.tdi` directory in the `<solution_directory>` to store the `com.ibm.di.server.autoload` property.
 - d Move the `TDI/QRadarIAM.xml` and `TDI/QRadarIAM.property` files from the Tivoli® Directory Integrator directory to `<solution_directory>/autoload.tdi` directory or the directory you created in the previous step.
 - e Move the `QradarIAM.bat` and `QradarIAM.sh` scripts from the Tivoli® Directory Integrator directory to the location from which you want to start the Tivoli® Directory Integrator.
- 6 If certificate-based authentication is required for your system to authenticate to the Tivoli® Directory Integrator, select one of the following options:
 - To create and import a self-signed certificate, see Step 7.
 - To import a CA certificate, see Step 8.
- 7 Create and import the self-signed certificate into the Tivoli® Directory Integrator truststore.
 - a To generate a keystore and a private/public key pair, type the following command:
 - `keytool -genkey -dname cn=<server_ip_address> -validity <days_valid> -keystore <keystore_file> -storepass <password> -keypass <password>`
 - For example, `keytool -genkey -dname cn=192.168.1.1 -validity 365 -keystore server.jks -storepass secret -keypass secret`
 - b To export the certificate from the keystore, type the following command:
 - `keytool -export -alias <alias> -file <certificate_file> -keystore <keystore_file> -storepass <password>`
 - For example, `keytool -export -alias mykey -file server.cert -keystore server.jks -storepass secret`
 - c To import the primary certificate back into the keystore as the self-signed CA certificate, type the following command:
 - `keytool -import -trustcacerts -file <certificate_file> -keystore <keystore_file> -storepass <password> -alias <alias>.`
 - For example, `keytool -import -trustcacerts -file server.cert -keystore server.jks -storepass secret -alias mytrustedkey`
 - d Copy the certificate file to the `/opt/qradar/conf/trusted_certificates` on the Extreme Security Console.

- 8 Import the CA certificate into the Tivoli® Directory Integrator truststore.
 - a To import the CA certificate into the keystore as the self-signed CA certificate, type the following command:
 - `keytool -import -trustcacerts -file <certificate_file> -keystore <keystore_file> -storepass <password> -alias <alias>.`
 - For example, `keytool -import -trustcacerts -file server.cert -keystore server.jks -storepass secret -alias mytrustedkey`
 - b Copy the CA certificate file to the `/opt/qradar/conf/trusted_certificates` on the Extreme Security Console.
- 9 Edit the `<solution_directory>/solution.properties` file to uncomment and configure the following properties:
 - `javax.net.ssl.trustStore=<keystore_file>`
 - `{protect}-javax.net.ssl.trustStorePassword=<password>`
 - `javax.net.ssl.keyStore=<keystore_file>`
 - `{protect}-javax.net.ssl.keyStorePassword=<password>`



Note

The default current, unmodified password might be displayed in the following format: `{encr}EyHbak`. Enter the password as plain text. The password is encrypted the first time that you start Tivoli® Directory Integrator.

Creating and managing user information source

Use the `UISConfigUtil` utility to create, retrieve, update, or delete user information sources.

Creating a user information source

Use the `UISConfigUtil` utility to create a user information source.

Before you create a user information source, you must install and configure your Tivoli® Directory Integrator server. For more information, see [Configuring the Tivoli Directory Integrator Server](#) on page 56.

When you create a user information source, you must identify the property values required to configure the user information source. The following table describes the supported property values:

Table 21: Supported user interface property values

Property	Description
<code>tdiserver</code>	Defines the host name of the Tivoli® Directory Integrator server.
<code>tdiport</code>	Defines the listening port for the HTTP connector on the Tivoli® Directory Integrator server.
<code>hostname</code>	Defines the host name of the user information source host.

Table 21: Supported user interface property values (continued)

Property	Description
port	Defines the listening port for the Identity and Access Management registry on the user information host.
username	Defines the user name that Log Manager uses to authenticate to the Identity and Access Management registry.
password	Defines the password that is required to authenticate to the Identity and Access Management registry.
searchbase	Defines the base DN.
search filter	Defines the search filter that is required to filter the user information that is retrieved from the Identity and Access Management registry.

- 1 Using SSH, log in to your Console as the root user.
 - a User name: `root`
 - b Password: `<password>`
- 2 To add a user information source, type the following command: `UISConfigUtil.sh add <name> -t <AD|ISAM|ISIM|ISFIM> [-d description] [-p prop1=value1,prop2=value2...,propn=valuen]`
 Where:
 - `<name>` Is the name of the user information source you want to add.
 - `<AD|ISAM|ISIM|ISFIM>` Indicates the user information source type.
 - `[-d description]` Is a description of the user information source. This parameter is optional.
 - `[-p prop1=value1,prop2=value2,...,propn=valuen]` Identifies the property values required for the user information source. For more information about the supported parameters, see [Creating a user information source](#) on page 58.

For example:

- ```
/UISConfigUtil.sh add "UIS_ISIM" -t ISIM -d "UIS for ISIM" -p
"tdiserver=nc9053113023.tivlab.austin.ibm.com,tdiport=8080,
hostname=vmibm7094.ottawa.ibm.com,port=389,
username=cn=root,password=password,\"searchbase=ou=org,DC=COM\",\\
\"searchfilter=(|(objectClass=erPersonItem)(objectClass=erBPPersonItem)
(objectClass=erSystemUser))\""
```

## Retrieving user information sources

Use the `UISConfigUtil` utility to retrieve user information sources.

- 1 Using SSH, log in to your Console as the root user.
  - a User name: `root`
  - b Password: `<password>`
- 2 Choose one of the following options:
  - a Type the following command to retrieve all user information sources: `UISConfigUtil.sh get <name>`

- b Type the following command to retrieve a specific user information source:

```
UISConfigUtil.sh get <name>
```

Where **<name>** is the name of the user information source you want to retrieve.

For example:

```
[root@vmibm7089 bin]# .UISConfigUtil.sh get "UIS_AD"
```

## Editing a user information source

Use the UISConfigUtil utility to edit a user information source.

- 1 Using SSH, log in to your Console as the root user.
  - a User name: **root**
  - b Password: **<password>**
- 2 Type the following command to edit a user information source: `UISConfigUtil.sh update <name> -t <AD|ISAM|ISIM|ISFIM> [-d description] [-p prop1=value1,prop2=value2,...,propn=valuen]`

Where:

- **<name>** Is the name of the user information source you want to edit.
- **<AD|ISAM|ISIM|ISFIM>** Indicates the user information source type. To update this parameter, type a new value.
- **[-d description]** Is a description of the user information source. This parameter is optional. To update this parameter, type a new description.
- **[-p prop1=value1,prop2=value2,...,propn=valuen]** Identifies the property values required for the user information source. To update this parameter, type **new properties**. For more information about the supported parameters, see [Creating a user information source](#) on page 58.

For example:

```
./UISConfigUtil.sh update "UIS_AD_update" -t AD -d "UIS for AD" -p "searchbase=DC=local"
```

## Deleting a user information source

Use the UISConfigUtil utility to delete a user information source.

- 1 Using SSH, log in to your Console as the root user.
  - a User name: **root**
  - b Password: **<password>**
- 2 Type the following command to delete a user information source: `UISConfigUtil.sh delete <name>`

Where **<name>** is the name of the user information source you want to delete.

The collected user information is stored in a reference data collection in the Extreme Networks Security Analytics database. If no reference data collection exists, a new reference data collection is created. If a

reference data collection was previously created for this user information source, the reference map is purged of previous data and the new user information is stored. For more information about reference data collections, see [Reference data collections](#).

## Collecting user information

Use the `GetUserInfo` utility to collect user information from the user information sources and store the data in a reference data collection.

Use this task to collect user information on demand. If you want to create automatic user information collection on a schedule, create a cron job entry. For more information about cron jobs, see your Linux™ documentation.

- 1 Using SSH, log in to your Console as the root user.
  - a User name: `root`
  - b `<password>`
- 2 Type the following command to collect user information on demand:  
`GetUserInfo.sh <UISName>`

Where `<UISName>` is the name of the user information source you want to collect information from.

The collected user information is stored in a reference data collection on the database. If no reference data collection exists, a new reference data collection is created. If a reference data collection was previously created for this user information source, the reference map is purged of previous data and the new user information is stored. For more information about reference data collections, see [Reference data collections for user information](#) on page 54.

# 6 Set up Extreme Security

---

Network hierarchy  
Automatic updates  
Set up a Extreme Security update server  
Configuring system settings  
Configuring your IF-MAP server certificates  
SSL certificate replacement in Extreme Security products  
IPv6 addressing in Extreme Security deployments  
Data retention  
Configuring system notifications  
Configuring a custom asset property  
Index management

Use the features on the **Admin** tab to set up Extreme Networks Security Log Manager.

You can configure your network hierarchy, automatic updates, system settings, event retention buckets, system notifications, console settings, and index management.

## Network hierarchy

---

Extreme Security uses the network hierarchy to understand your network traffic and provide you with the ability to view activity for your entire deployment.

When you develop your network hierarchy, consider the most effective method for viewing network activity. The network hierarchy does not need to resemble the physical deployment of your network. Extreme Security supports any network hierarchy that can be defined by a range of IP addresses. You can base your network on many different variables, including geographical or business units.

When you define your network hierarchy, you must consider the systems, users, and servers that can be grouped.

You can group systems and user groups that have similar behavior. However, do not group a server that has unique behavior with other servers on your network. Placing a unique server alone provides the server greater visibility in Extreme Security, and you can manage specific policies.

Within a group, you can place servers with high volumes of traffic, such as mail servers, at the top of the group. This hierarchy provides you with a visual representation when a discrepancy occurs.

You can organize your systems and networks by role or similar traffic patterns. For example, mail servers, departmental users, labs, or development groups. Using this organization, you can differentiate network behavior and enforce network management security policies.

Large network groups can cause you difficulty when you view detailed information for each object. Do not configure a network group with more than 15 objects.

Combine multiple Classless Inter-Domain Routings (CIDRs) or subnets into a single network group to conserve disk space. For example:

**Table 22: Example of multiple CIDRs and subnets in a single network group**

| Group | Description      | IP addresses                                 |
|-------|------------------|----------------------------------------------|
| 1     | Marketing        | 10.10.5.0/24                                 |
| 2     | Sales            | 10.10.8.0/21                                 |
| 3     | Database Cluster | 10.10.1.3/32<br>10.10.1.4/32<br>10.10.1.5/32 |

Add key servers as individual objects and group other major but related servers into multi-CIDR objects.

Define an all-encompassing group so when you define new networks, the appropriate policies, and behavioral monitors are applied. For example:

**Table 23: Example of an all-encompassing group**

| Group     | Subgroup                | IP address   |
|-----------|-------------------------|--------------|
| Cleveland | Cleveland miscellaneous | 10.10.0.0/16 |
| Cleveland | Cleveland Sales         | 10.10.8.0/21 |
| Cleveland | Cleveland Marketing     | 10.10.1.0/24 |

If you add a network to the example, such as 10.10.50.0/24, which is an HR department, the traffic displays as Cleveland-based and any rules you apply to the Cleveland group are applied by default.

## Acceptable CIDR values

Extreme Security accepts specific CIDR values.

The following table provides a list of the CIDR values that Extreme Security accepts:

**Table 24: Acceptable CIDR values**

| CIDR Length | Mask      | Number of Networks | Hosts         |
|-------------|-----------|--------------------|---------------|
| /1          | 128.0.0.0 | 128 A              | 2,147,483,392 |
| /2          | 192.0.0.0 | 64 A               | 1,073,741,696 |
| /3          | 224.0.0.0 | 32 A               | 536,870,848   |
| /4          | 240.0.0.0 | 16 A               | 268,435,424   |
| /5          | 248.0.0.0 | 8 A                | 134,217,712   |
| /6          | 252.0.0.0 | 4 A                | 67,108,856    |
| /7          | 254.0.0.0 | 2 A                | 33,554,428    |
| /8          | 255.0.0.0 | 1 A                | 16,777,214    |

**Table 24: Acceptable CIDR values (continued)**

| CIDR Length | Mask            | Number of Networks | Hosts     |
|-------------|-----------------|--------------------|-----------|
| /9          | 255.128.0.0     | 128 B              | 8,388,352 |
| /10         | 255.192.0.0     | 64 B               | 4,194,176 |
| /11         | 255.224.0.0     | 32 B               | 2,097,088 |
| /12         | 255.240.0.0     | 16 B               | 1,048,544 |
| /13         | 255.248.0.0     | 8 B                | 524,272   |
| /14         | 255.252.0.0     | 4 B                | 262,136   |
| /15         | 255.254.0.0     | 2 B                | 131,068   |
| /16         | 255.255.0.0     | 1 B                | 65,534    |
| /17         | 255.255.128.0   | 128 C              | 32,512    |
| /18         | 255.255.192.0   | 64 C               | 16,256    |
| /19         | 255.255.224.0   | 32 C               | 8,128     |
| /20         | 255.255.240.0   | 16 C               | 4,064     |
| /21         | 255.255.248.0   | 8 C                | 2,032     |
| /22         | 255.255.252.0   | 4 C                | 1,016     |
| /23         | 255.255.254.0   | 2 C                | 508       |
| /24         | 255.255.255.0   | 1 C                | 254       |
| /25         | 255.255.255.128 | 2 subnets          | 124       |
| /26         | 255.255.255.192 | 4 subnets          | 62        |
| /27         | 255.255.255.224 | 8 subnets          | 30        |
| /28         | 255.255.255.240 | 16 subnets         | 14        |
| /29         | 255.255.255.248 | 32 subnets         | 6         |
| /30         | 255.255.255.252 | 64 subnets         | 2         |
| /31         | 255.255.255.254 | none               | none      |
| /32         | 255.255.255.255 | 1/256 C            | 1         |

For example, a network is called a supernet when the prefix boundary contains fewer bits than the natural (or classful) mask of the network. A network is called a subnet when the prefix boundary contains more bits than the natural mask of the network:

- 209.60.128.0 is a class C network address with a mask of /24.
- 209.60.128.0 /22 is a supernet that yields:
  - 209.60.128.0 /24
  - 209.60.129.0 /24
  - 209.60.130.0 /24
  - 209.60.131.0 /24
- 192.0.0.0 /25

Subnet Host Range



0 192.0.0.1-192.0.0.126

1 192.0.0.129-192.0.0.254

- 192.0.0.0 /26

Subnet Host Range

0 192.0.0.1 - 192.0.0.62

1 192.0.0.65 - 192.0.0.126

2 192.0.0.129 - 192.0.0.190

3 192.0.0.193 - 192.0.0.254

- 192.0.0.0 /27

Subnet Host Range

0 192.0.0.1 - 192.0.0.30

1 192.0.0.33 - 192.0.0.62

2 192.0.0.65 - 192.0.0.94

3 192.0.0.97 - 192.0.0.126

4 192.0.0.129 - 192.0.0.158

5 192.0.0.161 - 192.0.0.190

6 192.0.0.193 - 192.0.0.222

7 192.0.0.225 - 192.0.0.254

#### Related Links

[Defining your network hierarchy](#)

## Automatic updates

You can automatically or manually update your configuration files to ensure that your configuration files contain the latest network security information.

### Automatic update requirements

The Console must be connected to the Internet to receive the updates. If your Console is not connected to the Internet, you must configure an internal update server for your Console to download the files from.

Update files are available for manual download from the following website: [Customer Support](http://www.extremenetworks.com/support/) (www.extremenetworks.com/support/)

To maintain the integrity of your current configuration and information, either replace your existing configuration files or integrate the updated files with your existing files.

After you install updates on your Console and deploy your changes, the Console updates its managed hosts if your deployment is defined in your deployment editor. For more information about the deployment editor, see [Deployment editor](#) on page 112.

## Description of updates

Update files can include the following updates:

- Configuration updates, which include configuration file changes, vulnerability, QID map, and security threat information updates.
- DSM updates, which include corrections to parsing issues, scanner changes, and protocol updates.
- Major updates, which include items such as updated JAR files.
- Minor updates, which include items such as more Online Help content or updated scripts.

## Automatic updates for high availability deployments

When you update your configuration files on a primary host and deploy your changes, the updates are automatically made on the secondary host. If you do not deploy your changes, the updates are made on the secondary host through an automated process that runs hourly.

## Frequency of automatic updates for new installations and upgrades

The default frequency of the automatic update is determined by the installation type and the Extreme Security version.

- If you upgrade from Extreme Security versions earlier than V7.2, the value to which the update frequency is set remains the same after the upgrade. By default, the update is set to weekly, but you can manually change the frequency.
- If you install a new installation of Extreme Security V7.2 or later, the default frequency of the update is daily. You can manually change the frequency.

### Related Links

[Set up a Extreme Security update server](#) on page 70

If your deployment includes a Extreme Security Console that is unable to access the Internet or you want to manually manage updates to your system, you can set up a Extreme Security update server to manage the update process.

## Viewing pending updates

Your system is preconfigured for weekly automatic updates. You can view the pending updates in the **Updates** window.

Your system needs to be operational long enough to retrieve the weekly updates. If no updates are displayed in the **Updates** window, either your system has not been in operation long enough to retrieve the weekly updates or no updates have been issued. If this occurs, you can manually check for new

updates. For more information about checking for new updates, see [Checking for new updates](#) on page 69.

The **Check for Updates** toolbar provides the following functions:

**Table 25: Check for Updates toolbar functions**

| Function              | Description                                                                                                                                                                                                                                                                                  |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Hide</b>           | Select one or more updates, and then click <b>Hide</b> to remove the selected updates from the Check for Updates page. You can view and restore the hidden updates on the <b>Restore Hidden Updates</b> page. For more information, see <a href="#">Restoring hidden updates</a> on page 70. |
| <b>Install</b>        | You can manually install updates. When you manually install updates, the installation process starts within a minute. For more information, see <a href="#">Manually installing automatic updates</a> on page 69.                                                                            |
| <b>Schedule</b>       | You can configure a specific date and time to manually install selected updates on your Console. Scheduling is useful when you want to schedule the update installation during off-peak hours. For more information, see <a href="#">Scheduling an update</a> on page 68.                    |
| <b>Unschedule</b>     | You can remove preconfigured schedules for manually installing updates on your Console. For more information, see <a href="#">Scheduling an update</a> on page 68.                                                                                                                           |
| <b>Search By Name</b> | You can locate a specific update by name.                                                                                                                                                                                                                                                    |
| <b>Next Refresh</b>   | This counter displays the amount of time until the next automatic refresh. The list of updates on the <b>Check for Updates</b> page automatically refreshes every 60 seconds. The timer is automatically paused when you select one or more updates.                                         |
| <b>Pause</b>          | Pauses the automatic refresh process. To resume automatic refresh, click <b>Play</b> .                                                                                                                                                                                                       |
| <b>Refresh</b>        | Refreshes the list of updates.                                                                                                                                                                                                                                                               |

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration**.
- 3 Click **Auto Update**.
- 4 To view details on an update, select the update.

## Configuring automatic update settings

You can customize the automatic update settings to change the frequency, update type, server configuration, and backup settings.

You can select the **Auto Deploy** to automatically deploy updates. If **Auto Deploy** is not selected, then you must manually deploy changes, from the **Dashboard** tab, after updates are installed.

You can select **Auto Restart Service** to allow automatic updates that require the user interface to restart. A user interface disruption occurs when the service restarts. Alternatively, you can manually install the updated from the **Check for Updates** window.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration**.
- 3 Click **Auto Update**.
- 4 On the navigation menu, click **Change Settings**.
- 5 On the **Basic** tab, select the schedule for updates.

- 6 In the **Configuration Updates** section, select the method that you want to use for updating your configuration files.
- 7 In the **DSM, Scanner, Protocol Updates** section, select an option to install updates.
- 8 In the **Major Updates** section, select an option for receiving major updates for new releases.
- 9 In the **Minor updates** section, select an option for receiving patches for minor system issues.
- 10 Select the **Auto Deploy** check box if you want to deploy update changes automatically after updates are installed.
- 11 Select the **Auto Restart Service** check box if you want to restart the user interface service automatically after updates are installed.
- 12 Click the **Advanced** tab.
- 13 In **Web Server** field, type the web server from which you want to obtain the updates.  
The default web server is <https://qmmunity.qilabs.com/>.
- 14 In the **Directory** field, type the directory location on which the web server stores the updates. The default directory is `autoupdates/`.
- 15 Optional: In the **Proxy Server** field, type the URL for the proxy server.  
The proxy server is required if the application server uses a proxy server to connect to the Internet.
- 16 In the **Proxy Username** field, type the user name for the proxy server.  
A user name is required if you are using an authenticated proxy.
- 17 In the **Proxy Password** field, type the password for the proxy server.  
A password is required if you are using an authenticated proxy.
- 18 Select the **Send Feedback** check box if you want to send feedback to us about the update.  
If errors occur during an update, feedback is automatically sent by a web form.
- 19 In the **Backup Retention Period** list, type or select the number of days that you want to store files that are replaced during the update process.  
The files are stored in the location that is specified in the **Backup Location**. The minimum is one day and the maximum is 65535 years.
- 20 In the **Backup Location** field, type the location where you want to store backup files.
- 21 In the **Download Path** field, type the directory path location to which you want to store DSM, minor, and major updates.  
The default directory path is `/store/configservices/staging/updates`.
- 22 Click **Save**.

## Scheduling an update

Automatic updates occur on a recurring schedule according to the settings on the **Update Configuration** page. You can also schedule an update or a set of updates to run at a specific time.

To reduce performance impacts on your system, schedule a large update to run during off-peak hours.

For detailed information on each update, you can select the update. A description and any error messages are displayed in the right pane of the window.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration**.
- 3 Click **Auto Update**.

- 4 Optional: If you want to schedule specific updates, select the updates that you want to schedule.
- 5 From the **Schedule** list box, select the type of update you want to schedule.
- 6 Using the calendar, select the start date and time of when you want to start your scheduled updates.

## Clearing scheduled updates

You can cancel any scheduled update.

Scheduled updates display a status of **Scheduled** in the **Status** field. After the schedule is cleared, the status of the update displays as **New**.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration**.
- 3 Click **Auto Update**.
- 4 On the navigation menu, click **Check for Updates**.
- 5 Optional: If you want to clear specific scheduled updates, select the updates that you want to clear.
- 6 From the **Unschedule** list box, select the type of scheduled update that you want to clear.

## Checking for new updates

Extreme Networks® provides updates on a regular basis. By default, the Auto Update feature is scheduled to automatically download and install updates. If you require an update at a time other than the preconfigured schedule, you can download new updates.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration**.
- 3 Click **Auto Update**.
- 4 On the navigation menu, click **Check for Updates**.
- 5 Click **Get new updates**.

## Manually installing automatic updates

Extreme Networks® provides updates regularly. By default, updates are automatically downloaded and installed on your system. However, you can install an update at a time other than the preconfigured schedule.

The system retrieves the new updates from Fix Central. This might take an extended period. When complete, new updates are listed on the **Updates** window.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration**.
- 3 Click **Auto Update**.
- 4 On the navigation menu, click **Check for Updates**.
- 5 Optional: If you want to install specific updates, select the updates that you want to schedule.
- 6 From the **Install** list box, select the type of update you want to install.

## Viewing your update history

After an update was successfully installed or failed to install, the update is displayed on the **View Update History** page.

A description of the update and any installation error messages are displayed in the right pane of the **View Update History** page. The **View Update History** page provides the following information:

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration**.
- 3 Click **Auto Update**.
- 4 On the navigation menu, click **View Update History**.
- 5 Optional: Using the **Search by Name** text box, you can type a keyword and then press Enter to locate a specific update by name.
- 6 To investigate a specific update, select the update.

## Restoring hidden updates

You can remove updates from the **Check for Updates** page. You can view and restore the hidden updates on the **Restore Hidden Updates** page.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration**.
- 3 Click **Auto Update**.
- 4 On the navigation menu, click **Restore Hidden Updates**.
- 5 Optional: To locate an update by name, type a keyword in the **Search by Name** text box and press Enter.
- 6 Select the hidden update that you want to restore.
- 7 Click **Restore**.

## Viewing the autoupdate log

The autoupdate log contains the most recent automatic update that was run on your system.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration**.
- 3 Click **Auto Update**.
- 4 On the navigation menu, click **View Log**.

## Set up a Extreme Security update server

If your deployment includes a Extreme Security Console that is unable to access the Internet or you want to manually manage updates to your system, you can set up a Extreme Security update server to manage the update process.

The autoupdate package includes all files necessary to manually set up an update server in addition to the necessary system configuration files for each update. After the initial setup, you only need to

download and uncompress the most current autoupdate package to manually update your configuration.

You can subscribe to notifications in Fix Central to receive notification of new updates.

## Related Links

[Automatic updates](#) on page 65

You can automatically or manually update your configuration files to ensure that your configuration files contain the latest network security information.

## Configuring your update server

Use this task to configure an Apache server. You must create an update directory and download the autoupdate package from Fix Central.

Autoupdates are available in Fix Central.

- 1 Access your Apache server.  
By default, the update directory is in the web root directory of the Apache server. You can place the directory in another location if you configure Extreme Security accordingly.
- 2 Create an update directory named `autoupdates/`.
- 3 Optional: Create an Apache user account and password to be used by the update process.
- 4 Download the autoupdate package from Fix Central: <http://www.ibm.com/support/fixcentral>  
You can find Extreme Security products in the Security Systems **Product Group** list on Fix Central.
- 5 Save the autoupdate package file on your Apache server in the `autoupdates/` directory that you created.
- 6 On the Apache server, type the following command to uncompress the autoupdate package: `tar -zxvf updatepackage-[timestamp].tgz`
- 7 Click the **Admin** tab.
- 8 On the navigation menu, click **System Configuration**.
- 9 Click **Auto Update**.
- 10 Click **Change Settings**.
- 11 Select the **Advanced** tab.
- 12 To direct the update process to the Apache server, configure the following parameters in the **Server Configuration** panel:
  - a In **Web Server** field, type the address or directory path of your Apache server.  
If the Apache server runs on non-standard ports, add `:<portnumber>` to the end of the address.  
`https://qmmunity.q1labs.com/:8080`
  - b In the **Directory** field, type the directory location on which the web server stores the updates.  
The default directory is `autoupdates/`.
  - c Optional: In the **Proxy Server** field, type the URL for the proxy server.  
The proxy server is required if the application server uses a proxy server to connect to the Internet.

- d Optional: In the **Proxy Username** field, type the user name for the proxy server.  
A user name is required if you are using an authenticated proxy.
  - e Optional: In the **Proxy Password** field, type the password for the proxy server.  
A password is required if you are using an authenticated proxy.
- 13 Select **Deploy changes**.
  - 14 Click **Save**.
  - 15 Using SSH, log in to Extreme Security as the root user.
  - 16 Type the following command to configure the user name that you set for your Apache server: `/opt/qradar/bin/UpdateConfs.pl -change_username <username>`
  - 17 Type the following command to configure the password that you set for your Apache server: `/opt/qradar/bin/UpdateConfs.pl -change_password <password>`
  - 18 Test your update server by typing the command: `lynx https://<your update server>/<directory path to updates>/manifest_list`
  - 19 Type the user name and password.

## Configuring your Extreme Security Console as the Update Server

You can configure your Extreme Security Console to be your update server.

To configure your Extreme Security console to be your update server, you complete three tasks:

- Create an autoupdate directory.
  - Download the autoupdate package from Fix Central.
  - Configure Extreme Security to accept the autoupdates.
- 1 Log in to Extreme Security as the root user.
  - 2 Type the following command to create the autoupdate directory: `mkdir /opt/qradar/www/autoupdates/`
  - 3 Download the autoupdate package from Fix Central: <http://www.ibm.com/support/fixcentral>  
You can find Extreme Security products in the Security Systems **Product Group** list on Fix Central.
  - 4 Save the autoupdate package file on your Apache server in the `autoupdates/` directory that you created.
  - 5 On your Extreme Security Console, type the following command to uncompress the autoupdate package: `tar -zxvf updatepackage-[timestamp].tgz`
  - 6 Log in to Extreme Security user interface.
  - 7 On the navigation menu, click **System Configuration**.
  - 8 Click **Auto Update**.
  - 9 Click **Change Settings**.
  - 10 Select the **Advanced** tab.
  - 11 In **Web Server** field, type `https://localhost/`.
  - 12 Clear the **Send feed** check box.

## Adding new updates

You can download updates from Fix Central to your update server.



You must configure your update server and set up Extreme Security to receive updates from the update server.

- 1 Download the autoupdate package from Fix Central: <http://www.ibm.com/support/fixcentral>  
You can find Extreme Security products in the Security Systems **Product Group** list on Fix Central.
- 2 Save the autoupdate package file on your update server in the `autoupdates/` directory that you created.
- 3 Type the following command to uncompress the autoupdate package: `tar -zxf autoupdate-[timestamp].tgz`.
- 4 Log in to Extreme Security as the root user.
- 5 Type the following command to test your update server, `lynx https://<your update server>/<directory path to updates>/manifest_list`.
- 6 Type the user name and password of your update server.

## Configuring system settings

You can configure common system settings on the **System Settings** window.

The **System Settings** window includes configurable parameters for the following system settings:

- System settings
- Database settings
- Ariel database settings
- SNMP settings
- Embedded SNMP daemon settings
- Asset profile settings
- Console settings
- Authentication settings
- DNS settings
- WINS settings
- Reporting settings
- Data export settings

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration**.
- 3 Click the **System Settings** icon.
- 4 Configure the system settings.
- 5 Click **Save**.
- 6 On the **Admin** tab menu, select **Advanced > Deploy Full Configuration**.  
When you deploy the full configuration, Extreme Security restarts all services. Data collection for events stops until the deployment completes.

## Customizing the right-click menu

To provide quick access to functions, customize menu options by using a plug-in application programming interface (API). For example, you can add more menu items, such as an option to scan the NetBIOS.

The `ip_context_menu.xml` file accepts `menuEntry` XML nodes to customize the right-click menu.

```
<menuEntry name="{Name}" description="{Description}" exec="{Command}"
url="{URL}" requiredCapabilities="{Required Capabilities}"/>
```

The following list describes the attributes in the `menuEntry` element:

|                              |                                                                                                                                                                                                                                                                                                |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Name</b>                  | The text that is displayed in the right-click menu.                                                                                                                                                                                                                                            |
| <b>Description</b>           | The description of the entry. The description text is displayed in the tooltip for your menu option. The description is optional.                                                                                                                                                              |
| <b>URL</b>                   | Specifies the web address that opens in a new window. You can use the placeholder <code>%IP%</code> , to represent the IP address. To pass other URL parameters to this URL, you must use the <code>&amp;amp;</code> option, for example, <code>url="/lookup?&amp;ip=%IP%;force=true"</code> . |
| <b>Command</b>               | A command that you want to run on the Console. The output of the command is displayed in a new window. Use the placeholder, <code>%IP%</code> , to represent the IP address that is selected.                                                                                                  |
| <b>Required Capabilities</b> | Any capabilities, for example, "ADMIN", that the user must have before they select this option, comma-delimited. (for example, "ADMIN"). If the user does not have all capabilities that are listed, the entries are not displayed. Required capabilities is an optional field.                |

The edited file must look similar to the following example:

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- This is a configuration file to add custom actions into
the IP address right-click menu. Entries must be of one of the
following formats: -->
<contextMenu>
<menuEntry name="Traceroute" exec="/usr/sbin/traceroute %IP%" />
<menuEntry name="External ARIN Lookup"
url="http://ws.arin.net/whois/?queryinput=%IP%" />
</contextMenu>
```

- 1 Using SSH, log in to Extreme Networks Security Analytics as the root user.
- 2 On the Extreme Security server, copy the `ip_context_menu.xml` file from the `/opt/qradar/conf/templates` directory to the `/opt/qradar/conf` directory.
- 3 Open the `/opt/qradar/conf/ip_context_menu.xml` file for editing.
- 4 Edit the attributes in the `menuEntry` element.
- 5 Save and close the file.
- 6 To restart services, type the following command:

```
service tomcat restart
```

## Enhancing the right-click menu for event columns

You can add more actions to the right-click options that are available on the columns in the **Log Activity** table. For example, you can add an option to view more information about the source IP or destination IP.

You can pass any data that is in the event to the URL or script.



### Note

You can add options to the right-click menu on only the Extreme Security Console appliance and to only some Ariel database fields.

- 1 Using SSH, log in to the QRadar® Console appliance as the root user.
- 2 Go to the `/opt/qradar/conf` directory and create a file that is named `arielRightClick.properties`.
- 3 Edit the `/opt/qradar/conf/arielRightClick.properties` file. Use the following table to specify the parameters that determine the options for the **right-click** menu.  
The following table describes the parameters that you can use to customize the right-click menu.

**Table 27: Description of the `arielRightClick.properties` file parameters**

Parameter	Requirement	Description	Example
<code>pluginActions</code>	Required	Indicates either a URL or script action.	
<code>arielProperty</code>	Required	Specifies the column, or Ariel field name, for which the right-click menu is enabled.	<code>sourceIP</code> <code>sourcePort</code> <code>destinationIP</code> <code>qid</code>
<code>text</code>	Required	Specifies the text that is displayed on the <b>right click</b> menu.	Google search
<code>useFormattedValue</code>	Optional	Specifies whether formatted values are passed to the script. Set to <b>true</b> to ensure that the formatted value for attributes, such as <code>username</code> and <code>payload</code> , are passed. Formatted values are easier for administrators to read than unformatted values.	If the parameter is set to true for the event name (QID) property, the event name of the QID is passed to the script. If the parameter is set to false, the raw, unformatted QID value is passed to the script.
<code>url</code>	Required to access a URL	Specifies the URL, which opens in a new window, and the parameters to pass to the URL. Use the format: <code>\$Ariel_Field Name\$</code>	<code>sourceIPwebUrlAction.url=http://www.mywebsite.com?q=\$sourceIP\$</code>
<code>command</code>	Required if the action is a command	Specifies the absolute path of the command or script file.	<code>destinationPortScriptAction.command=/bin/echo</code>
<code>arguments</code>	Required if the action is a command	Specifies the data to pass to the script. Use the following format: <code>\$Ariel_Field Name\$</code>	<code>destinationPortScriptAction.arguments=\$qid\$</code>

For each of the key names that are specified in the `pluginActions` list, define the action by using a key with the format `key name, property`.

- 4 Save and close the file.
- 5 Log in to the QRadar® user interface.
- 6 Click the **Admin** tab.
- 7 Select **Advanced > Restart Web Server**.

The following example shows how to add `Test URL` as a right-click option for source IP addresses.

```
pluginActions=sourceIPwebUrlAction
sourceIPwebUrlAction.arielProperty=sourceIP
```

```
sourceIPwebUrlAction.text=Test URL
sourceIPwebUrlAction.url=http://www.mywebsite.com?q=$sourceIP$
```

The following example shows how to enable script action for destination ports.

```
pluginActions=destinationPortScriptAction

destinationPortScriptAction.arielProperty=destinationPort
destinationPortScriptAction.text=Test Unformatted Command
destinationPortScriptAction.useFormattedValue=false
destinationPortScriptAction.command=/bin/echo
destinationPortScriptAction.arguments=qid
```

The following example shows adding several parameters to a URL or a scripting action.

```
pluginActions=qidwebUrlAction,sourcePortScriptAction

qidwebUrlAction.arielProperty=qid,device,eventCount
qidwebUrlAction.text=Search on Google
qidwebUrlAction.url=http://www.google.com?q=qid-$device$-$eventCount$

sourcePortScriptAction.arielProperty=sourcePort
sourcePortScriptAction.text=Port Unformatted Command
sourcePortScriptAction.useFormattedValue=true
sourcePortScriptAction.command=/bin/echo
sourcePortScriptAction.arguments=qid-$sourcePort$-$device$-$CONTEXT$
```

## Asset retention values overview

Additional information for the period, in days, that you want to store the asset profile information.

- Assets are tested against the retention thresholds at regular intervals. By default, the cleanup interval is 12 hours
- All specified retention periods are relative to the last seen date of the information, regardless of whether the information was last seen by a scanner or passively observed by the system.
- Asset information is deleted as it expires, meaning that following a cleanup interval, all asset information within its retention threshold remains.
- By default, assets that are associated with un-remediated vulnerabilities (as detected by QVM or other scanner) are retained.
- Assets can always be deleted manually through the UI.

**Table 28: Asset components**

Asset component	Default retention (in days)	Notes
IP Address	120 days	By default, user-supplied IP Addresses are retained until they are deleted manually.
MAC Addresses (Interfaces)	120 days	By default, user-supplied interfaces are retained until they are deleted manually.

**Table 28: Asset components (continued)**

Asset component	Default retention (in days)	Notes
DNS and NetBIOS Hostnames	120 days	by default, user-supplied hostnames are retained until they are deleted manually.
Asset Properties	120 days	<p>By default, user-supplied IP Addresses are retained until they are deleted manually. the asset properties this value can affect are:</p> <ul style="list-style-type: none"> <li>• Given Name</li> <li>• Unified Name</li> <li>• Weight</li> <li>• Description</li> <li>• Business Owner</li> <li>• Business Contact</li> <li>• Technical Owner</li> <li>• Technical Contact</li> <li>• Location</li> <li>• Detection Confidence</li> <li>• Wireless AP</li> <li>• Wireless SSID</li> <li>• Switch ID</li> <li>• Switch Port ID</li> <li>• CVSS Confidentiality Requirement</li> <li>• CVSS Integrity Requirement</li> <li>• CVSS Availability Requirement</li> <li>• CVSS Collateral Damage Potential</li> <li>• Technical User</li> <li>• User Supplied OS</li> <li>• OS Override Type</li> <li>• OS Override Id</li> <li>• Extended</li> <li>• Legacy (Pre-7.2) Cvss Risk</li> <li>• VLAN</li> <li>• Asset Type</li> </ul>
Asset Products	120 days	<p>By default, user-supplied products are retained until they are deleted manually. Asset products include the following:</p> <ul style="list-style-type: none"> <li>• Asset OS</li> <li>• Asset Installed Applications</li> <li>• Products that are associated with open asset ports</li> </ul>
Asset "Open" Ports	120 days	

**Table 28: Asset components (continued)**

Asset component	Default retention (in days)	Notes
Asset netBIOS Groups	120 days	NetBIOS groups are seldom used, and more customers may not be aware of their existence. In the case where they are used, they are deleted after 120 days.
Asset Client Application	120 days	Client Applications are not yet leveraged in the UI. This value can be ignored.
Asset Users	30 days	

## Configuring your IF-MAP server certificates

Before you can configure IF-MAP authentication on the System Settings window, you must configure your IF-MAP server certificate.

### Configuring IF-MAP Server Certificate for Basic Authentication

This task provides instruction for how to configure your IF-MAP certificate for basic authentication.

Contact your IF-MAP server administrator to obtain a copy of the IF-MAP server public certificate. The certificate must have the `.cert` file extension, for example, `ifmapserver.cert`.

- 1 Using SSH, log in to Extreme Security as the root user.
- 2 Copy the certificate to the `/opt/qradar/conf/trusted_certificates` directory.

### Configuring IF-MAP Server Certificate for Mutual Authentication

This task provides instruction for how to configure your IF-MAP certificate for mutual authentication.

Contact your IF-MAP server administrator to obtain a copy of the IF-MAP server public certificate. The certificate must have the `.cert` file extension, for example, `ifmapserver.cert`.

Mutual authentication requires certificate configuration on your Console and your IF-MAP server. For assistance configuring the certificate on your IF-MAP server, contact your IF-MAP server administrator.

- 1 Using SSH, log in to Extreme Security as the root user.
- 2 Access the certificate to the `/opt/qradar/conf/trusted_certificates` directory
- 3 Copy the SSL intermediate certificate and SSL Verisign root certificate to your IF-MAP server as CA certificates. For assistance, contact your IF-MAP server administrator.
- 4 Type the following command to create the Public-Key Cryptography Standards file with the `.pkcs12` file extension using the following command:
 

```
openssl pkcs12 -export -inkey <private_key> -in <certificate> -out <pkcs12_filename.pkcs12> -name "IFMAP Client"
```
- 5 Type the following command to copy the `pkcs12` file to the `/opt/qradar/conf/key_certificates` directory:
 

```
cp <pkcs12_filename.pkcs12> /opt/qradar/conf/key_certificates
```

- 6 Create a client on the IF-MAP server with the Certificate authentication and upload the SSL certificate. For assistance, contact your IF-MAP server administrator.
- 7 Change the permissions of the directory by typing the following commands:  
`chmod 755 /opt/gradar/conf/trusted_certificates`  
`chmod 644 /opt/gradar/conf/trusted_certificates/*.cert`
- 8 Type the following command to restart the Tomcat service:  
`service tomcat restart`

## SSL certificate replacement in Extreme Security products

By default, Extreme Networks Security Analytics products provide an untrusted SSL certificate. You can replace the untrusted SSL certificate with either a self-signed or trusted certificate.

### SSL certificates overview

Secure Sockets Layer (SSL) is a security protocol that provides communication privacy. With SSL, client/server applications can communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery.

SSL is an industry standard and is used by websites to protect online transactions. To generate an SSL link, a web server requires an SSL certificate. SSL certificates are issued by software or trusted third-party certifying authorities.

### Trusted root

Browsers and operating systems include a preinstalled list of trusted certificates, which are installed in the Trusted Root Certification Authorities store. Extreme Security products trust any certificate that is signed by a trusted root CA.

### SSL Connections between Extreme Security components

To establish all internal SSL connections between components, Extreme Security does not trust certificates that are issued by a recognized authority. Instead, you must use the web server certificate that is preinstalled on the Extreme Security Console.

## Replacing the default SSL certificate

Replace the untrusted SSL certificate in Extreme Networks Security Analytics with either a self-signed certificate or a certificate that is issued by a trusted third-party certificate authority.

SSL certificates that are issued from some vendors, such as VeriSign, require an intermediate certificate. You must download the intermediate certificate from the vendor and use it during the configuration.

All trusted certificates for Extreme Security must meet the following requirements:

- The certificate must be a X.509 certificate and have PEM base64 encoding.
- The certificate must have a `.cert`, `.crt`, or `.der` file extension.

- Keystore files that contain certificates must have the `.truststore` file extension.
  - The certificate file must be stored in the `/opt/qradar/conf/trusted_certificates` directory.
- 1 Obtain a certificate from a trusted certificate authority.
  - 2 Use SSH to log in to your Extreme Security Console as the root user.
  - 3 To install the certificate, type the following command:  
`/opt/qradar/bin/install_ssl_cert.sh -i`
  - 4 Type the location of your private key file.  
Do not encrypt the private key when you install or replace an SSL certificate.
  - 5 If you are using an intermediate certificate, type the location of your public key file and the location of your intermediate certificate.
  - 6 To continue, type `Y` and press Enter.

## Generating a private/public RSA key pair

To obtain a trusted certificate, you must generate a public/private RSA key pair.

- 1 Type the following command:

```
ssh-keygen -t rsa
```

If you want to use DSA keys, you need to use the `ssh-keygen -t dsa` command.

- 2 Type the file in which to save the key or accept the default location.



### Note

The default file is `/root/.ssh/id_rsa`.

- 3 Type a passphrase.
- 4 Type the passphrase again.

If you accepted the default file location, the identification is `/root/.ssh/id_rsa`. Your public key is `/root/.ssh/id_rsa.pub`.

The key fingerprint is as follows:

```
0b:33:bb:76:1e:54:a8:48:d0:c8:b3:f9:31:41:77:e6 root@qradar.com
```

The random art image is as follows:

```
+--[RSA 2048]-----+
| ..+. . o |
| +.O. + . |
| +.. E . |
| o.O. . . |
| ..O= S |
| . * . |
| . o |
| |
| ..O. |
+-----+
```



In the .ssh file, there are three files:

- `id_rsa id_rsa.pub know_hosts`
- `rsa.pub` is the public key
- `rsa.id` is the private key

Send the private key to get the certificate and then you are returned a new public key and an intermediate key.

## IPv6 addressing in Extreme Security deployments

IPv4 and IPv6 addressing is supported for network connectivity and management of Extreme Networks Security Analytics software and appliances. When you install QRadar, you are prompted to specify whether your Internet Protocol is IPv4 or IPv6.

Review the following details about IPv6 addressing.

[Extreme Security components that support IPv6 addressing](#) on page 81

[Deploying Extreme Security in IPv6 or mixed environments](#) on page 82

[IPv6 addressing limitations](#) on page 82

### Extreme Security components that support IPv6 addressing

The following Extreme Security components support IPv6: addressing.

<b>Log Activity tab</b>	<p>Because <b>IPv6 Source Address</b> and <b>IPv6 Destination Address</b> are not default columns, they are not automatically displayed. To display these columns, you must select them when you configure your search parameters (column definition).</p> <p>When an address does not exist, template-based records are used to avoid wasted space. DSMs can parse IPv6 addresses from the event payload. If any DSM cannot parse IPv6 addresses, a log source extension can parse the addresses. For more information about log source extensions, see the <i>Log Sources Users Guide</i>.</p>
<b>Searching, grouping, and reporting on IPv6 fields</b>	<p>You can search events by using IPv6 parameters in the search criteria.</p> <p>You can also group and sort event records that are based on IPv6 parameters.</p> <p>You can create reports that are based on data from IPv6-based searches.</p>
<b>Custom rules</b>	<p>The following custom rule to support IPv6 addressing was added: <b>SRC/DST IP = IPv6 Address</b></p> <p>IPv6-based building blocks are available in other rules.</p>
<b>Deployment editor</b>	<p>The deployment editor supports IPv6 addresses.</p>
<b>Device support modules (DSMs)</b>	<p>DSMs can parse IPv6 source and destination address from event payloads.</p>

## Deploying Extreme Security in IPv6 or mixed environments

To log in to Extreme Security in an IPv6 or mixed environment, wrap the IP address in square brackets:

```
https://[<IP Address>]
```

Both IPv4 and IPv6 environments can use a hosts file for address translation. In an IPv6 or mixed environment, the client resolves the Console address by its host name. You must add the IP address of the IPv6 console to the `/etc/hosts` file on the client.

Event sources, such as syslog and SNMP, are accepted from IPv4 and IPv6 addresses.



### Note

By default, you cannot add an IPv4-only managed host to an IPv6 and IPv4 mixed-mode console. You must run a script to enable an IPv4-only managed host.

## IPv6 addressing limitations

When QRadar is deployed in an IPv6 environment, the following limitations are known:

- The network hierarchy is not updated to support IPv6.

Some parts of the Extreme Security deployment, including surveillance, searching, and analysis, do not take advantage of the network hierarchy. For example, within the Log Activity tab, you cannot search or aggregate events By Network

- No IPv6-based asset profiles.
- Asset profiles are created only if Extreme Security receives events, and vulnerability data for IPv4 hosts.
- No host profile test in custom rules for IPv6 addresses.
- No specialized indexing or optimization of IPv6 addresses.

## Installing an IPv4-only managed host in a mixed environment

By default, in Extreme Networks Security Analytics products, you cannot add an IPv4-only managed host to an IPv6 and IPv4 mixed-mode console. You must run a script to enable an IPv4-only managed host.

- 1 Install the Extreme Security Console by selecting IPv6 addressing.
- 2 After installation, on the Extreme Security Console, type the following command:  
`/opt/qradar/bin/setup_v6v4_console.sh`
- 3 To add an IPv4 managed host, type the following command:  
`/opt/qradar/bin/add_v6v4_host.sh`
- 4 Add the managed host by using the deployment editor.

## Data retention

Configure custom retention periods for specific data.

Retention buckets define retention policies for events that match custom filter requirements. As Extreme Security receives events, each event is compared against retention bucket filter criteria. When an event matches a retention bucket filter, it is stored in that retention bucket until the retention policy time period is reached. This feature enables you to configure multiple retention buckets.

Retention buckets are sequenced in priority order from the top row to the bottom row on the Event Retention window. A record is stored in the bucket that matches the filter criteria with highest priority. If the record does not match any of your configured retention buckets, the record is stored in the default retention bucket, which is always located below the list of configurable retention buckets.

## Configuring retention buckets

By default, the Event Retention window provide a default retention bucket and 10 unconfigured retention buckets. Until you configure a retention bucket, all events are stored in the default retention bucket.

The Event Retention window provide the following information for each retention bucket:

**Table 29: Retention window parameters**

Parameter	Description
Order	The priority order of the retention buckets.
Name	The name of the retention bucket.
Retention	The retention period of the retention bucket.
Compression	The compression policy of the retention bucket.
Deletion Policy	The deletion policy of the retention bucket.
Filters	The filters applied to the retention bucket. Move your mouse pointer over the <b>Filters</b> parameter for more information on the applied filters.
Distribution	The retention bucket usage as a percentage of total data retention in all your retention buckets.
Enabled	Specifies if the retention bucket is enabled (true) or disabled (false).
Creation Date	The date and time the retention bucket was created.
Modification Date	The date and time the retention bucket was last modified.

The toolbar provides the following functions:

**Table 30: Retention window toolbar**

Function	Description
Edit	Edit a retention bucket.
Enable/Disable	Enable or disable a retention bucket. When you disable a bucket, any new data that matches the requirements for the disabled bucket are stored in the next bucket that matches the properties.
Delete	Delete a retention bucket. When you delete a retention bucket, the data contained in the retention bucket is not removed from the system, only the criteria defining the bucket is deleted. All data is maintained in storage.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **Data Sources**.
- 3 Click the **Event Retention** icon.
- 4 Double-click the first available retention bucket.
- 5 Configure the following parameters:

<i>Parameter</i>	<i>Description</i>
Name	Type a unique name for the retention bucket.
Keep data placed in this bucket for	Select a retention period. When the retention period is reached, data is deleted according to the <i>Delete data in this bucket</i> parameter.
Allow data in this bucket to be compressed	Select the check box to enable data compression, and then select a time frame from the list box. When the time frame is reached, all data in the retention bucket are eligible to be compressed. This increases system performance by guaranteeing that no data is compressed within the specified time period. Compression only occurs when used disk space reaches 83% for payloads and 85% for records.
Delete data in this bucket	<p>Select a deletion policy.</p> <p>Select <b>When storage space is required</b> if you want data that matches the <i>Keep data placed in this bucket for</i> parameter to remain in storage until the disk monitoring system detects that storage is required. If used disk space reaches 85% for records and 83% for payloads, data will be deleted. Deletion continues until the used disk space reaches 82% for records and 81% for payloads.</p> <p>Select <b>Immediately after the retention period has expired</b> if you want data to be deleted immediately on matching the <i>Keep data placed in this bucket for</i> parameter. The data is deleted at the next scheduled disk maintenance process, regardless of free disk space or compression requirements.</p> <p>When storage is required, only data that matches the <i>Keep data placed in this bucket for</i> parameter are deleted.</p>
Description	Type a description for the retention bucket.
Current Filters	<p>Configure your filters.</p> <p>From the first list, select a parameter you want to filter for. For example, Device, Source Port, or Event Name.</p> <p>From the second list, select the modifier you want to use for the filter. The list of modifiers depends on the attribute selected in the first list.</p> <p>In the text field, type specific information related to your filter and then click <b>Add Filter</b>. The filters are displayed in the <b>Current Filters</b> text box. You can select a filter and click <b>Remove Filter</b> to remove a filter from the <b>Current Filter</b> text box.</p>

- 6 Click **Save**.
- 7 Click **Save** again.

Your retention bucket starts storing data that match the retention parameters immediately.

## Managing retention bucket sequence

You can change the order of the retention buckets to ensure that data is being matched against the retention buckets in the order that matches your requirements.

Retention buckets are sequenced in priority order from the top row to the bottom row on the Event Retention window. A record is stored in the first retention bucket that matches the record parameters.

You cannot move the default retention bucket. It always resides at the bottom of the list.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **Data Sources**.
- 3 Click the **Event Retention** icon.
- 4 Click the icon.
- 5 Select and move the required retention bucket to the correct location.

## Editing a retention bucket

If required, you can edit the parameters of a retention bucket.

On the Retention Parameters window, the Current Filters pane is not displayed when editing a default retention bucket.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **Data Sources**.
- 3 Choose one of the following options:
- 4 Click the **Event Retention** icon.
- 5 Select the retention bucket you want to edit, and then click **Edit**.
- 6 Edit the parameters. For more information see, [Configuring retention buckets](#) on page 83.
- 7 Click **Save**.

## Enabling and disabling a retention bucket

When you configure and save a retention bucket, it is enabled by default. You can disable a bucket to tune your event retention.

When you disable a bucket, any new events that match the requirements for the disabled bucket are stored in the next bucket that matches the event properties.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **Data Sources**.
- 3 Choose one of the following options:
- 4 Click the **Event Retention** icon.
- 5 Select the retention bucket you want to disable, and then click **Enable/Disable**.

## Deleting a Retention Bucket

When you delete a retention bucket, the events contained in the retention bucket are not removed from the system, only the criteria defining the bucket is deleted. All events are maintained in storage.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **Data Sources**.
- 3 Click the **Event Retention** icon.
- 4 Select the retention bucket you want to delete, and then click **Delete**.

## Configuring system notifications

You can configure system performance alerts for thresholds. This section provides information about configuring your system thresholds.

The following table describes the Global System Notifications window parameters

**Table 31: Global System Notifications window parameters**

Parameter	Description
System load over 1 minute	Type the threshold system load average over the last minute.
System load over 5 minutes	Type the threshold system load average over the last 5 minutes.
System load over 15 minutes	Type the threshold system load average over the last 15 minutes.
Percentage of swap used	Type the threshold percentage of used swap space.
Received packets per second	Type the threshold number of packets received per second.
Transmitted packets per second	Type the threshold number of packets transmitted per second.
Received bytes per second	Type the threshold number of bytes received per second.
Transmitted bytes per second	Type the threshold number of bytes transmitted per second.
Receive errors	Type the threshold number of corrupted packets received per second.
Transmit errors	Type the threshold number of corrupted packets transmitted per second.
Packet collisions	Type the threshold number of collisions that occur per second while transmitting packets.
Dropped receive packets	Type the threshold number of received packets that are dropped per second due to a lack of space in the buffers.
Dropped transmit packets	Type the threshold number of transmitted packets that are dropped per second due to a lack of space in the buffers.
Transmit carrier errors	Type the threshold number of carrier errors that occur per second while transmitting packets.
Receive frame errors	Type the threshold number of frame alignment errors that occur per second on received packets.
Receive fifo overruns	Type the threshold number of First In First Out (FIFO) overrun errors that occur per second on received packets.
Transmit fifo overruns	Type the threshold number of First In First Out (FIFO) overrun errors that occur per second on transmitted packets.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration**.
- 3 Click the **Global System Notifications** icon.
- 4 Enter values for each parameter that you want to configure.

- 5 For each parameter, select **Enabled** and **Respond if value is** and then select one of the following options:

Option	Description
<b>Greater Than</b>	An alert occurs if the parameter value exceeds the configured value.
<b>Less Than</b>	An alert occurs if the parameter value is less than the configured value.

- 6 Type a description of the preferred resolution to the alert.
- 7 Click **Save**.
- 8 On the tab menu, click **Deploy Changes**.

## Configuring custom email notifications

When you configure rules in QRadar, specify that each time the rule generates a response, an email notification is sent to recipients. The email notification provides useful information, such as event properties.

You can customize the content that is included in the email notification for rule response by editing the `alert-config.xml` file.



### Note

References to flows do not apply to QRadar Log Manager.

You must create a temporary directory where you can safely edit your copy of the files, without the risk of overwriting the default files. After you edit and save the `alert-config.xml` file, you must run a script that validates your changes. The validation script automatically applies your changes to a staging area, from where you can deploy by using the QRadar deployment editor.

- 1 Using SSH, log in to the QRadar Console as the root user.
- 2 Create a new temporary directory to use to safely edit copies of the default files.
- 3 To copy the files that are stored in the `custom_alerts` directory to the temporary directory, type the following command:

```
cp /store/configservices/staging/globalconfig/templates/
custom_alerts/*.* <directory_name>
```

The `<directory_name>` option is the name of the temporary directory that you created.

- 4 Confirm that the files were copied successfully:
  - a To list the files in the directory, type the following command:
 

```
ls -lah
```
  - b Verify that the following file is listed:
 

```
alert-config.xml
```
- 5 Open the `alert-config.xml` file for editing.

- 6 To create multiple template elements, copy the `<template></template>` element, including tags and the contents, and then paste it below the existing `<template></template>` element.

**note**

Although you can add multiple template elements, you can set the `Active` property to `True` in only one event template type.

- 7 Edit the contents of the `<template></template>` element:
  - a Specify the template type by using the following XML property:
 

```
<templatetype></templatetype>
```

This value is mandatory.
  - b Specify the template name by using the following XML element:
 

```
<templatename></templatename>
```
  - c Set the active element to true:
 

```
<active>true</active>
```
  - d Edit the subject element, if required.
  - e Add or remove parameters from the body element. For valid parameters, see the [Accepted Parameters](#) table.
  - f Repeat these steps for each template that you add.
- 8 Save and close the file.
- 9 To validate your changes, type the following command:

```
/opt/qradar/bin/runCustAlertValidator.sh <directory_name>
```

The `<directory_name>` option is the name of the temporary directory that you created.

If the script validates the changes successfully, the following message is displayed:

```
File alert-config.xml was deployed successfully to staging!
```

- 10 Log in to QRadar.
- 11 Click the **Admin** tab.
- 12 Select **Advanced > Deploy Full Configuration**.

When you deploy the full configuration, Extreme Security restarts all services. Data collection for events stops until the deployment completes.

**Table 32: Accepted Notification Parameters**

Common Parameters	Event Parameters	Flow Parameters
AppName	EventCollectorID	Type
RuleName	DeviceId	CompoundAppID
RuleDescription	DeviceName	FlowSourceIDs
EventName	DeviceTime	SourceASNList
EventDescription	DstPostNATPort	DestinationASNList
EventProcessorId	SrcPostNATPort	InputIFIndexList



**Table 32: Accepted Notification Parameters (continued)**

Common Parameters	Event Parameters	Flow Parameters
Qid	DstMACAddress	OutputIFIndexList
Category	DstPostNATIPAddress	Appld
RemoteDestinationIP	DstPreNATIPAddress	Host
Payload	SrcMACAddress	Port
Credibility	SrcPostNATIPAddress	SourceBytes
Relevance	SrcPreNATIPAddress	SourcePackets
Source	SrcPreNATPor	Direction
SourcePort	DstPreNATPort	SourceTOS
SourceIP		SourceDSCP
Destination		SourcePrecedence
DestinationPort		DestinationTOS
DestinationIP		DestinationDSCP
DestinationUserName		SourceASN
Protocol		DestinationASN
StartTime		InputIFIndex
Duration		OutputIFIndex
StopTime		FirstPacketTime
EventCount		LastPacketTime
SourceV6		TotalSourceBytes
DestinationV6		TotalDestinationBytes
UserName		TotalSourcePackets
DestinationNetwork		TotalDestinationPackets
SourceNetwork		SourceQOS
Severity		DestinationQOS
CustomPropertiesList		SourcePayload

## Configuring a custom asset property

Define asset properties to facilitate asset queries. Custom properties provide more query options.

- 1 Click the **Admin** tab.
- 2 Click **Custom Asset Properties**.
- 3 In the **Name** field, enter a descriptor for the custom asset property.
- 4 In the **Type** drop-down menu, select **Numeric** or **Text** to define the information type for the custom asset property.
- 5 Click **OK**.

- 6 Click the **Assets** tab.
- 7 Click **Edit Asset > Custom Asset Properties**.
- 8 Enter the required information in the value field.
- 9 Click **OK**.

## Index management

The Index Management feature allows you to control database indexing on event properties.

Indexing event properties allows you to optimize your searches. You can enable indexing on any property that is listed in the Index Management window and you can enable indexing on more than one property.

The Index Management feature also provides statistics, such as:

- The percentage of saved searches running in your deployment that include the indexed property
- The volume of data that is written to the disk by the index during the selected time frame

To enable payload indexing, you must enable indexing on the Quick Filter property.

## Enabling indexes

The Index Management window lists all event properties that can be indexed and provides statistics for the properties. Toolbar options allow you to enable and disable indexing on selected event properties.

Modifying database indexing might decrease system performance. Ensure that you monitor the statistics after you enable indexing on multiple properties.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click *System Configuration*.
- 3 Click the **Index Management** icon.
- 4 Select one or more properties from the Index Management list.
- 5 Choose one of the following options:
  - Click **Enable Index**.
  - Click **Disable Index**.
- 6 Click **Save**.
- 7 Click **OK**.

In lists that include event properties, indexed property names are appended with the following text: *[Indexed]*. Examples of such lists include the search parameters on the *Log Activity* tab search criteria pages and the Add Filter window.

## Enabling payload indexing to optimize search times

To optimize event search times, enable payload indexing on the **Quick Filter** property.

### Note

Use the **Quick Filter** feature in the **Log Activity** tab to search event payloads by using a text string.



Payload indexing increases disk storage requirements and might affect system performance. Enable payload indexing if your deployment meets the following conditions:

- The event processors are at less than 70% disk usage.
- The event processors are less than 70% of the maximum events per second (EPS) rating.

- 1 From the navigation pane on the **Admin** tab in the Extreme Security product, click **System Configuration**.

- 2 Click **Index Management**.

- 3 In the **Quick Search** field, type **Quick Filter**.

The **Quick Filter** property is displayed.

- 4 Select the **Quick Filter** property that you want to index.

In the results table, use the value in the **Database** column to identify the events **Quick Filter** property.

- 5 On the toolbar, click **Enable Index**.

A green dot indicates that the payload index is enabled.

If a list includes event properties that are indexed, the property names are appended with the following text: [ **Indexed** ].

- 6 Click **Save**.

To manage payload indexes, see [Configuring the retention period for payload indexes](#) on page 91.

## Configuring the retention period for payload indexes

You can configure the time period that Extreme Networks Security Analytics products store payload indexes.

By default, payload indexes are retained for one week. The minimum retention period one day and the maximum is two years.

- 1 Click the **Admin** tab.

- 2 On the navigation menu, click **System Configuration**.

- 3 Click **System Settings**.

- 4 In the **Database Settings** section, select a retention time period from the **Payload Index Retention** list.

- 5 Click **Save**.

- 6 Close the **System Settings** window.

- 7 On the **Admin** tab menu, click **Deploy Changes**.

# 7 Reference data management

Adding reference data collections  
Editing reference data collections  
Deleting reference data collections  
Viewing reference data collection contents  
Adding an element to reference data collections  
Deleting elements from reference data collections  
Importing elements into reference data collections  
Exporting elements from reference data collections  
Manage reference data collections with the reference data utility

Use reference data collections to store, retrieve, and test complex data structures. Using the **Reference Data Management** window, you can create and manage reference data. You can also import elements into reference data collections from an external file.

You can use the **Reference Data Management** window to manage the following reference data collection types:

<b>Reference Set</b>	<p>A reference set is a set of elements that are derived from events that occur on your network. Examples of elements that are derived from events are IP addresses or user names.</p> <p>After you create a reference set, you can create rules to detect log activity that is associated with the reference set. For example, you can create a rule to detect when an unauthorized user attempts to access your network resources. You can also configure a rule to add an element to a reference set when log activity matches the rule conditions. For example, you can create a rule to detect when an employee accesses a prohibited website and add that employee's IP address to a reference set. For more information on configuring rules, see the <i>Users Guide</i> for your product.</p>
<b>Reference map</b>	<p>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.</p>
<b>Reference map of sets</b>	<p>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.</p>
<b>Reference map of maps</b>	<p>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.</p>



## Note

Reference map of maps can only be managed by using the reference data command line utility.

- Reference table** A Reference table is a representation of values using a combination of two keys (key1 and key2). key1 can map to multiple key2s. Each key2 has a direct mapping to a value. This mapping enables a single key1 to be mapped to multiple key2-value pairs in the Reference table data structure.
- For example, to test for network bandwidth violations, you can configure the Reference Table to store relevant information, such as the 'Application', 'User' and 'Time of Violation' for each source IP. In this case, use the Source IP property for key1, which you can then map to multiple key2 parameters.
- The 'Application' generating this traffic is the first key2 and the value stores the *Application* parameter.
  - The 'User' is the second key2 and the value stores the *Username* parameter.
  - The 'Time of Violation' is the third key2 and the value stores the *Start Time* parameter.

## Adding reference data collections

From the **Admin** tab, you can add reference data collections that you can include in rule tests.

After you create a reference data collection, it is listed on the **Reference Data Management** window. In the Rule wizard, the reference data collection is listed as an option on the **Rule Response** page. After you configure one or more rules to send elements to the reference data collection, the **Number of Elements**, and **Associated Rules** parameters are automatically updated.

- 1 On the **Reference Data Management** window, click **Add**.
- 2 Select the reference data collection type that you want to add.
- 3 Configure the parameters:

**Table 33: Reference data parameters**

Parameter	Description
<b>Name</b>	A unique name for this reference set. The maximum length is 255 characters
<b>Type</b>	If you selected <b>Reference Set</b> , <b>Reference Map</b> , or <b>Reference Map of Sets</b> , you must define the data type that you want to employ. You cannot edit the <b>Type</b> parameter after you configure your reference data.
<b>Key Parameters</b>	If you selected <b>Reference Table</b> , you must define key parameters by clicking <b>Add Parameter</b> and adding key names and selecting a data type in the relevant columns.
<b>Time to Live of Elements</b>	The amount of time that you want to maintain each element in the reference data. <b>Lives Forever</b> is the default setting. If you specify an amount of time, you must also indicate when you want to start tracking time for an element by selecting the <b>Since first seen</b> or <b>Since last seen</b> radio button.

- 4 Click **Create**.

## Editing reference data collections

Use the **Reference Data Management** window to edit reference data element Time to Live parameters.

- 1 In the **Reference Data Management** window, select a reference data collection type.
- 2 Click **Edit**.
- 3 Edit the Time to Live parameters.

- 4 Click **Submit**.

## Deleting reference data collections

You can delete a reference set or reference data collection from the **Reference Data Management** window.

When you delete reference data collections, a confirmation window indicates whether the reference data collections that you want to delete have rules or search criteria dependencies that are associated with them. After you delete a reference data collection, the configuration is cleared from the associated rules.



### Tip

Before you delete a reference data collection, you can view associated rules in the **Reference** tab in the **Reference Data Editor** window.

Choose one of the following options:

- On the **Reference Data Management** window, select a reference data collection, and then click **Delete**.
- On the **Reference Data Management** window, use the **Quick Search** text box to display only the reference sets or reference data collections that you want to delete, and then click **Delete Listed**.

## Viewing reference data collection contents

The **Content** tab provides a list of the elements that are included in this reference data collection.

- 1 On the **Reference Data Management** window, select a reference data collection.
- 2 Click **View Contents**.
- 3 To view contents, click the **Content** tab in the **Reference Data Editor** window.



### Tip

Use the **Quick Search** field to filter for specific elements. All elements that match the keyword are listed in the **Content** list. Then, you can select the action from the toolbar.

**Table 34: Content tab parameters**

Parameter	Description
	The value of Key 1 for maps, maps of sets, maps of maps, and reference data tables. This column is hidden for reference sets.
	The value of Key 2 for maps of maps, and reference data tables. This column is hidden for all reference data types except maps of maps, and reference data tables.
<b>Value</b>	The value of the element. For example, if the reference contains a list of IP addresses, the value is the IP address.
<b>Origin</b>	The <b>rulename</b> is placed in the reference set as a response to a rule. The <b>User</b> is imported from an external file or manually added to the reference set.

**Table 34: Content tab parameters (continued)**

Parameter	Description
Time to Live	The time that is remaining until this element is removed from the reference set.
Date Last Seen	The date and time that this element was last detected on your network.

- Click the **References** tab and view the references.

**Table 35: References tab parameters**

Parameter	Description
Rule Name	The name of this rule.
Group	The name of the group this rule belongs to.
Category	The category of the rule. Options include <b>Custom Rule</b> or <b>Anomaly Detection Rule</b> .
Type	The type of this rule.
Enabled	Indicates whether the rule is enabled or disabled.
Response	The responses that are configured for this rule.
Origin	<b>System</b> indicates a default rule. <b>Modified</b> indicates that a default rule was customized. <b>User</b> indicates a user-created rule.

- To view or edit an associated rule, double-click the rule in the **References** list, or select it and click **Edit**. Alternatively,  
In the Rule wizard, you can edit the rule configuration settings.

## Adding an element to reference data collections

You add an element to a reference data collection by using the **Reference Data Management** window.

- On the **Reference Data Management** window, select a reference data collection type.
- Click **View Contents**.
- Click the **Content** tab.
- On the toolbar, click **Add**.
- Configure the following parameters:

Parameter	Description
Key 1	The value of Key 1 for maps, maps of sets and reference data tables. This field is hidden for reference sets.
Key 2	The value of Key 2 for reference data tables. This field is hidden for all reference data collection types except reference data tables.
Value(s)	If you want to type multiple values, include a separator character between each value, and then specify the separator character in the <b>Separator Character</b> field.
Separator Character	Type the separator character that you used in the <b>Value(s)</b> field.

- 6 Click **Add**.

## Deleting elements from reference data collections

You can delete elements from a reference data collection.

- 1 On the **Reference Data Management** window, select a reference data collection.
- 2 Click **View Contents**.
- 3 Click the **Content** tab.
- 4 Choose one of the following options:
  - Select an element, and then click **Delete**.
  - Use the **Quick Search** text box to display only the elements that you want to delete, and then click **Delete Listed**.
- 5 Click **Delete**.

## Importing elements into reference data collections

You can import elements from an external CSV or text file.

Ensure that the CSV or text file that you want to import is stored on your local desktop.



### Note

Extreme Networks Security Analytics imports notes in CSV or text files as values.

- 1 On the **Reference Data Management** window, select a reference data collection.
- 2 Click **View Contents**.
- 3 Click the **Content** tab.
- 4 On the toolbar, click **Import**.
- 5 Click **Browse**.
- 6 Select the CSV or text file that you want to import.
- 7 Click **Import**.

## CSV file requirements for reference data collections

If you plan to import an external file containing data elements into a reference data collection, ensure that the file is in Comma Separated Value (CSV) format. Also, ensure that you copied the CSV file to your system.

The CSV file must follow the format in the examples reference data collections. The # symbol in the first column indicates a comment line. The first non-comment line is the column header and identifies the column name (ie., **key1**, **key2**, **data**). Then each non-commented line that follows is a data record that is added to the map. Keys are alphanumeric strings.

*Example 1: Reference map*

```
#
#
ReferenceMap
```



```
#
key1,data
key1,value1
key2,value2
```

*Example 2: Reference map of sets*

```
#
#
ReferenceMapOfSets
#
key1,data
key1,value1
key1,value2
```

*Example 3: Reference map of maps*

```
#
#
ReferenceMapOfMaps
#
key1,key2,data
map1,key1,value1
map1,key2,value2
```



#### Note

Reference map of maps can only be managed by using the reference data command line utility.

*Example 3: Reference table*

```
#
#
ReferenceTable
#
key1,key2,type,data
map1,key1,type1,value1
map1,key2,type 1,value2
```

## Exporting elements from reference data collections

You can export reference data collection elements to an external CSV or text file.

- 1 On the **Reference Data Management** window, select a reference data collection.
- 2 Click **View Contents**.
- 3 Click the **Content** tab.
- 4 On the toolbar, click **Export**.
- 5 Choose one of the following options:
- 6 If you want to open the list for immediate viewing, select the **Open with** option and select an application from the list box.
- 7 If you want to save the list, select the **Save File** option.

- 8 Click **OK**.

## Manage reference data collections with the reference data utility

Use the `ReferenceDataUtil.sh` utility to make complex reference data collections.

Use the reference data utility to manage reference data collections from the command line. You can use `ReferenceDataUtil.sh` to create the following reference data collection types:

- Reference map
- Reference map of sets
- Reference map of maps
- Reference table

### Creating a reference data collection with the reference data utility

Use the `ReferenceDataUtil.sh` utility to create a reference data collection.

- 1 Using SSH, log in to Extreme Security as the root user.

- 2 Go to the `/opt/qradar/bin` directory.

- 3 To create the reference data collection, type the following command:

```
./ReferenceDataUtil.sh create name [MAP | MAPOFSETS | MAPOFMAPS |
REFTABLE] [ALN | NUM | IP | PORT | ALNIC | DATE] [-
timeoutType=[FIRST_SEEN | LAST_SEEN]] [-TIMETOLIVE=]
```

- 4 To populate the map with data from an external file, type the following command:

```
./ReferenceDataUtil.sh load name filename [-encoding=...] [-sdf=" ...
"]
```

Create an Alphanumeric Map

```
./ReferenceDataUtil.sh create testALN MAP ALN
```

Create a Map of Sets of PORT values that will age out 3 hours after they were last seen

```
./ReferenceDataUtil.sh create testPORT MAPOFSETS PORT -timeoutType=LAST_SEEN
-timeToLive='3 hours'
```

Create a Map of Maps of Numeric values that will age out 3 hours 15 minutes after they were first seen

```
./ReferenceDataUtil.sh create testNUM MAPOFMAPS NUM -timeoutType=FIRST_SEEN
-timeToLive='3 hours 15 minutes'
```

Create a ReferenceTable with a default of Alphanumeric values

```
./ReferenceDataUtil.sh create testTable REFTABLE ALN
-keyType=ipKey:IP,portKey:PORT,numKey:NUM,dateKey:DATE
```

Log in to the user interface to create rules that add data to your reference data collections. You can also create rule tests that detect activity from elements that are in your reference data collection. For more information about creating rules and rule tests, see the *Users Guide* for your product.

## ReferenceDataUtil.sh command reference

You can manage your reference data collections using the `ReferenceDataUtil.sh` utility.

### *create*

Creates a reference data collection.

### *update*

Updates a reference data collection.

### *add*

Adds a data element to a reference data collection

### *delete*

Deletes an element from a reference data collection.

### *remove*

Removes a reference data collection.

### *purge*

Purges all elements from a reference data collection.

### *list*

Lists elements in a reference data collection.

### *listall*

Lists all elements in all reference data collection.

### *load*

Populates a reference data collections with data from an external CSV file.

# 8 Managing authorized services

Viewing authorized services  
Adding an authorized service  
Revoking authorized services

You can configure authorized services on the **Admin** tab to authenticate an API call for your Extreme Security deployment.

The Extreme Security RESTful API uses authorized services to authenticate API calls to the Extreme Security Console. For more information about the RESTful API, see the *Extreme Networks Security API Reference Guide*.

The **Manage Authorized Services** window provides the following information:

**Table 36: Parameters for authorized services**

Parameter	Description
Service Name	The name of the authorized service.
Authorized By	The name of the user or administrator that authorized the addition of the service.
Authentication Token	The token that is associated with this authorized service.
User Role	The user role that is associated with this authorized service.
Security Profile	The security profile that is associated with this authorized service.
Created	The date that this authorized service was created.
Expires	The date and time that the authorized service expires. By default, the authorized service is valid for 30 days.

## Viewing authorized services

The **Authorized Services** window displays a list of authorized services, from which you can copy the token for the service.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration**.
- 3 Click **Authorized Services**.
- 4 From the **Manage Authorized Services** window, select the appropriate authorized service.

The token is displayed in the **Selected Token** field in the top bar. You can copy the token into your vendor software to authenticate with Extreme Security.

## Adding an authorized service

---

Use the **Add Authorized Service** window to add a new authorized service.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration**.
- 3 Click **Authorized Services**.
- 4 Click **Add Authorized Service**.
- 5 In the **Service Name** field, type a name for this authorized service. The name can be up to 255 characters in length.
- 6 From the **User Role** list, select the user role that you want to assign to this authorized service. The user roles that are assigned to an authorized service determine the functions that this service can access on the Extreme Security user interface.
- 7 From the **Security Profile** list, select the security profile that you want to assign to this authorized service. The security profile determines the networks and log sources that this service can access on the Extreme Security user interface.
- 8 In the **Expiry Date** list, type or select a date that you want this service to expire. If an expiry date is not required, select **No Expiry**.
- 9 Click **Create Service**.

The confirmation message contains a token field that you must copy into your vendor software to authenticate with Extreme Networks Security Analytics.

## Revoking authorized services

---

Use the **Add Authorized Service** window to revoke an authorized service.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration**.
- 3 Click **Authorized Services**.
- 4 From the **Manage Authorized Services** window, select the service that you want to revoke.
- 5 Click **Revoke Authorization**.

# 9 Manage backup and recovery

## Backup archive management

### Backup archive creation

### Backup archive restoration

You can back up and recover Extreme Security configuration information and data.

You can use the backup and recovery feature to back up your event data; however, you must restore event data manually. For assistance in restoring your event data, see the *Restoring Your Data Technical Note*.

By default, Extreme Security creates a backup archive of your configuration information daily at midnight. The backup archive includes configuration information, data, or both from the previous day.

You can use two types of backups; configuration backups and data backups.

Configuration backups include the following components:

- Assets
- Certificates
- Custom logos
- Custom rules
- Device Support Modules (DSMs)
- Event categories
- Groups
- Index management information
- License key information
- Log sources
- Store and Forward schedules
- User and user roles information
- Vulnerability data (if Extreme Security Vulnerability Manager is installed)

Data backups include the following information:

- Audit log information
- Event data
- Report data
- Indexes
- Reference set elements

## Backup archive management

View and manage backup archives

From the **Backup Management Archive** window, you can view and manage all successful backup archives.

### Viewing backup archives

Use the **Backup Archives** window to view a list of your backup archives.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration**.
- 3 Click **Backup and Recovery**.

### Importing a backup archive

Importing a backup archive is useful if you want to restore a backup archive that was created on another Extreme Security host.

If you place a Extreme Security backup archive file in the `/store/backupHost/inbound` directory on the Console server, the backup archive file is automatically imported.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration**.
- 3 Click the **Backup and Recovery** icon.
- 4 In the **Upload Archive** field, click **Browse**.
- 5 Locate and select the archive file that you want to upload. The archive file must include a .tgz extension.
- 6 Click **Open**.
- 7 Click **Upload**.

### Deleting a backup archive

To delete a backup archive file, the backup archive file and the Host Context component must be located on the same system. The system must also be in communication with the Console and no other backup can be in progress.

If a backup file is deleted, it is removed from the disk and from the database. Also, the entry is removed from this list and an audit event is generated to indicate the removal.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration**.
- 3 Click **Backup and Recovery**.
- 4 In the **Existing Backups** section, select the archive that you want to delete.
- 5 Click **Delete**.

## Backup archive creation

By default, Extreme Security creates a backup archive of your configuration information daily at midnight. The backup archive includes your configuration information, data, or both from the previous day. You can customize this nightly backup and create an on-demand configuration backup, as required.

### Scheduling nightly backup

Use the **Backup Recovery Configuration** window to configure a night scheduled backup process.

By default, the nightly backup process includes only your configuration files. You can customize your nightly backup process to include data from your Console and selected managed hosts. You can also customize your backup retention period, backup archive location, the time limit for a backup to process before timing out, and the backup priority in relation to other Extreme Security processes.

The Backup Recovery Configuration window provides the following parameters:

**Table 37: Backup Recovery Configuration parameters**

Parameter	Description
General Backup Configuration	
Backup Repository Path	<p>Type the location where you want to store your backup file. The default location is <code>/store/backup</code>. This path must exist before the backup process is initiated. If this path does not exist, the backup process aborts.</p> <p>If you modify this path, make sure the new path is valid on every system in your deployment.</p> <ul style="list-style-type: none"> <li>Active data is stored on the <code>/store</code> directory. If you have both active data and backup archives stored in the same directory, data storage capacity might easily be reached and your scheduled backups might fail. We recommend you specify a storage location on another system or copy your backup archives to another system after the backup process is complete. You can use a Network File System (NFS) storage solution in your Extreme Security deployment. For more information on using NFS, see the <i>Extreme Networks Security Offboard Storage Guide</i>.</li> </ul>
Backup Retention Period (days)	<p>Type or select the length of time, in days, that you want to store backup files. The default is 2 days.</p> <p>This period of time only affects backup files generated as a result of a scheduled process. On-demand backups or imported backup files are not affected by this value.</p>
Nightly Backup Schedule	Select a backup option.
Select the managed hosts you would like to run data backups:	<p>This option is only displayed if you select the <b>Configuration and Data Backups</b> option.</p> <p>All hosts in your deployment are listed. The first host in the list is your Console; it is enabled for data backup by default, therefore no check box is displayed. If you have managed hosts in your deployment, the managed hosts are listed below the Console and each managed host includes a check box.</p> <p>Select the check box for the managed hosts you want to run data backups on.</p> <p>For each host (Console or managed hosts), you can optionally clear the data items you want to exclude from the backup archive.</p>
Configuration Only Backup	



**Table 37: Backup Recovery Configuration parameters (continued)**

Parameter	Description
Backup Time Limit (min)	Type or select the length of time, in minutes, that you want to allow the backup to run. The default is 180 minutes. If the backup process exceeds the configured time limit, the backup process is automatically canceled.
Backup Priority	From this list box, select the level of importance that you want the system to place on the configuration backup process compared to other processes. A priority of medium or high have a greater impact on system performance.
<i>Data Backup</i>	
Backup Time Limit (min)	Type or select the length of time, in minutes, that you want to allow the backup to run. The default is 1020 minutes. If the backup process exceeds the configured time limit, the backup is automatically canceled.
Backup Priority	From the list, select the level of importance you want the system to place on the data backup process compared to other processes. A priority of medium or high have a greater impact on system performance.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration**.
- 3 Click the **Backup and Recovery**.
- 4 On the toolbar, click **Configure**.
- 5 On the **Backup Recovery Configuration** window, customize your nightly backup.
- 6 Click **Save**.
- 7 Close the **Backup Archives** window.
- 8 On the **Admin** tab menu, click **Deploy Changes**.

## Creating an on-demand configuration backup archive

If you must back up your configuration files at a time other than your nightly scheduled backup, you can create an on-demand backup archive. On-demand backup archives include only configuration information.

You initiate an on-demand backup archive during a period when Extreme Security has low processing load, such as after normal office hours. During the backup process, system performance is affected.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration**.
- 3 Click **Backup and Recovery**.
- 4 From the toolbar, click **On Demand Backup**.

- 5 Enter values for the following parameters:

Option	Description
Name	Type a unique name that you want to assign to this backup archive. The name can be up to 100 alphanumeric characters in length. The name can contain following characters: underscore (_), dash (-), or period (.).
Description	Type a description for this configuration backup archive. The description can be up to 255 characters in length.

- 6 Click **Run Backup**.

You can start a new backup or restore processes only after the on-demand backup is complete. You can monitor the backup archive process in the **Backup Archives** window. See [Viewing backup archives](#) on page 103.

## Backup archive restoration

Restoring a backup archive is useful if you want to restore previously archived configuration files and asset data on your Extreme Security system.

Before you restore a backup archive, note the following considerations:

- You can only restore a backup archive created within the same release of software, including the patch level. For example, if you are running Extreme Networks Security Analytics 7.1.0 (MR2), the backup archive must have been created in Extreme Networks Security Analytics.
- The restore process only restores your configuration information, offense data, and asset data. For assistance in restoring your event data, see the *Restoring Your Data* Technical Note.
- If the backup archive originated on a NATed Console system, you can only restore that backup archive on a NATed system.

During the restore process, the following steps are taken on the Console:

- 1 Existing files and database tables are backed up.
- 2 Tomcat is shut down.
- 3 All system processes are shut down.
- 4 Files are extracted from the backup archive and restored to disk.
- 5 Database tables are restored.
- 6 All system processes are restarted.
- 7 Tomcat restarts.

## Restoring a backup archive

You can restore a backup archive. Restoring a backup archive is useful if you have a system hardware failure or you want to store a backup archive on a replacement appliance.

You can restart the Console only after the restore process is complete.

The restore process can take up to several hours; the process time depends on the size of the backup archive that must be restored. When complete, a confirmation message is displayed.

A window provides the status of the restore process. This window provides any errors for each host and instructions for resolving the errors.

The following parameters are available in the Restore a Backup window:

**Table 38: Restore a Backup parameters**

Parameter	Description
<b>Name</b>	The name of the backup archive.
<b>Description</b>	The description, if any, of the backup archive.
<b>Type</b>	The type of backup. Only configuration backups can be restored, therefore, this parameter displays <b>config</b> .
<b>Select All Configuration Items</b>	When selected, this option indicates that all configuration items are included in the restoration of the backup archive.
<b>Restore Configuration</b>	Lists the configuration items to include in the restoration of the backup archive. To remove items, you can clear the check boxes for each item you want to remove or clear the <b>Select All Configuration Items</b> check box.
<b>Select All Data Items</b>	When selected, this option indicates that all data items are included in the restoration of the backup archive.
<b>Restore Data</b>	Lists the configuration items to include in the restoration of the backup archive. All items are cleared by default. To restore data items, you can select the check boxes for each item you want to restore.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration**.
- 3 Click the **Backup and Recovery**.
- 4 Select the archive that you want to restore.
- 5 Click **Restore**.
- 6 On the **Restore a Backup** window, configure the parameters.
- 7 Click **Restore**.
- 8 Click **OK**.
- 9 Click **OK**.
- 10 Choose one of the following options:
  - If the user interface was closed during the restore process, open a web browser and log in to Extreme Security.
  - If the user interface was not closed, the login window is displayed. Log in to Extreme Security.
- 11 Follow the instructions on the status window.

After you verify that your data is restored to your system, ensure that your DSMs, vulnerability assessment (VA) scanners, and log source protocols are also restored.

If the backup archive originated on an HA cluster, you must click **Deploy Changes** to restore the HA cluster configuration after the restore is complete. If disk replication is enabled, the secondary host immediately synchronizes data after the system is restored. If the secondary host was removed from the deployment after a backup, the secondary host displays a failed status on the **System and License Management** window.

## Restoring a backup archive created on a different Extreme Security system

Each backup archive includes the IP address information of the system from which the backup archive was created. When you restore a backup archive from a different Extreme Security system, the IP address of the backup archive and the system that you are restoring are mismatched. You can correct the mismatched IP addresses.

You can restart the Console only after the restore process is complete.

The restore process can take up to several hours; the process time depends on the size of the backup archive that must be restored. When complete, a confirmation message is displayed.

A window provides the status of the restore process. This window provides any errors for each host and instructions for resolving the errors.

You must stop the iptables service on each managed host in your deployment. The Iptables service is a Linux™ based firewall.

The Restore a Backup (Managed Hosts Accessibility) window provides the following information.

**Table 39: Restore a Backup (Managed Host Accessibility) parameters**

Parameter	Description
Host Name	The managed host name.
IP Address	The IP address of the managed host.
Access Status	The access status to the managed host.

The Restore a Backup window provides the following parameters:

**Table 40: Restore a Backup parameters**

Parameter	Description
Name	The name of the backup archive.
Description	The description, if any, of the backup archive.
Type	The type of backup. Only configuration backups can be restored, therefore, this parameter displays <b>config</b> .
Select All Configuration Items	When selected, this option indicates that all configuration items are included in the restoration of the backup archive. This check box is selected by default. To clear all configuration items, clear the check box.
Restore Configuration	Lists the configuration items to include in the restoration of the backup archive. All items are selected by default. To remove items, you can clear the check boxes for each item you want to remove or clear the <b>Select All Configuration Items</b> check box.
Select All Data Items	When selected, this option indicates that all data items are included in the restoration of the backup archive. This check box is selected by default. To clear all data items, clear this check box.
Restore Data	Lists the configuration items to include in the restoration of the backup archive. All items are cleared by default. To restore data items, you can select the check boxes for each item you want to restore.

- 1 Click the **Admin** tab.

- 2 On the navigation menu, click **System Configuration**.
- 3 Click the **Backup and Recovery**.
- 4 Select the archive that you want to restore.
- 5 Click **Restore**.
- 6 On the **Restore a Backup** window, configure the parameters.
- 7 Click **Restore**.
- 8 Stop the IP tables:
  - a Using SSH, log in to the managed host as the root user.
  - b Type the command, `service iptables stop`.
  - c Repeat for all managed hosts in your deployment.
- 9 On the **Restore a Backup** window, click **Test Hosts Access**.
- 10 After testing is complete for all managed hosts, verify that the status in the **Access Status** column indicates a status of **OK**.
- 11 If the **Access Status** column indicates a status of **No Access** for a host, stop iptables again, and then click **Test Host Access** again to attempt a connection.
- 12 On the **Restore a Backup** window, configure the parameters.
- 13 Click **Restore**.
- 14 Click **OK**.
- 15 Click **OK** to log in.
- 16 Choose one of the following options:
  - If the user interface was closed during the restore process, open a web browser and log in to Extreme Security.
  - If the user interface was not closed, the login window is displayed. Log in to Extreme Security.
- 17 View the results of the restore process and follow the instructions to resolve any errors.
- 18 Refresh your web browser window.
- 19 From the **Admin** tab, select **Advanced > Deploy Full Configuration**.
 

When you deploy the full configuration, Extreme Security restarts all services. Data collection for events stops until the deployment completes.

After you verify that your data is restored to your system, you must reapply RPMs for any DSMs, vulnerability assessment (VA) scanners, or log source protocols.

If the backup archive originated on an HA cluster, you must click **Deploy Changes** to restore the HA cluster configuration after the restore is complete. If disk replication is enabled, the secondary host immediately synchronizes data after the system is restored. If the secondary host was removed from the deployment after a backup, the secondary host displays a failed status on the **System and License Management** window.

## Restoring data

You can restore the data on your Extreme Security Console and managed hosts from backup files. The data portion of the backup files includes information such as source and destination IP address information, asset data, event category information, vulnerability data, and event data.

Each managed host in your deployment, including the Extreme Security Console, creates all backup files in the `/store/backup/` directory. Your system might include a `/store/backup` mount from

an external SAN or NAS service. External services provide long term, offline retention of data, which is commonly required for compliancy regulations, such as PCI.



#### Note

You must restore the configuration backup before you restore the data backup.

Ensure that the following conditions are met:

- If you are restoring data on a new Extreme Security Console, the configuration backup is restored.
- You know the location of the managed host where the data is backed up.
- If your deployment includes a separate mount point for that volume, the `/store` or `/store/ariel` directory has sufficient space for the data that you want to recover.
- You know the date and time for the data that you want to recover.

- 1 Using SSH, log in to Extreme Security as the root user.
- 2 Go to the `/store/backup` directory.
- 3 To list the backup files, type `ls -l`
- 4 If backup files are listed, go to the root directory by typing `cd /`



#### Note

The restored files must be in the `/store` directory. If you type `cd` instead of `cd /`, the files are restored to the `/root/store` directory.

- 5 To extract the backup files to their original directory, type the following command:

```
tar -zxpvPf /store/backup/backup.<name>.<hostname_hostID>
.<target date>.<backup type>.<timestamp>.tgz
```

**Table 41: Description of file name variables**

File name variable	Description
<i>hostname_hostID</i>	The name of the Extreme Security system that hosts the backup file followed by the identifier for the Extreme Security system
<i>target date</i>	The date that the backup file was created. The format of the target date is <code>&lt;day&gt;_&lt;month&gt;_&lt;year&gt;</code>
<i>backup type</i>	The options are <b>data</b> or <b>config</b>
<i>timestamp</i>	The time that the backup file was created.

Daily backup of data captures all data on each host. If you want to restore data on a managed host that contains only event data, only that data is restored to that host.

## Verifying restored data

Verify that your data is restored correctly in Extreme Networks Security Analytics.

- 1 To verify that the files are restored, review the contents of one of the restored directories by typing the following command:

```
cd /store/ariel/events/payloads/<yyyy/mm/dd>
```

You can view the restored directories that are created for each hour of the day. If directories are missing, data might not be captured for that time period.

- 2 Verify that the restored data is available.
  - a Log in to the Extreme Security interface.
  - b Click the **Log Activity** tab.
  - c Select **Edit Search** from the **Search** list on the toolbar.
  - d In the **Time Range** pane of the **Search** window, select **Specific Interval**.
  - e Select the time range of the data you restored and then click **Filter**.
  - f View the results to verify the restored data.
  - g If your restored data is not available in the Extreme Security interface, verify that data is restored in the correct location and file permissions are correctly configured.

Restored files must be in the `/store` directory. If you typed `cd` instead of `cd /` when you extracted the restored files, check the `/root/store` directory for the restored files. If you did not change directories before you extracted the restored files, check the `/store/backup/store` directory for the restored files.

Typically, files are restored with the original permissions. However, if the files are owned by the root user account, issues might occur. If the files are owned by the root user account, change the permissions by using the `chown` and `chmod` commands.

After you verified that your data is restored, you must reapply RPMs for any DSMs, vulnerability assessment (VA) scanners, and log source protocols.

# 10 Deployment editor

- Deployment editor requirements
- Deployment editor views
- Building your deployment using the Deployment Editor
- Generating public keys for Extreme Security products
- Event view management
- Viewing the progress of data rebalancing
- Archiving Data Node content
- Saving event processor data to a Data Node appliance
- System view management
- NAT management
- Component configuration

Use the deployment editor to manage the individual components of your Extreme Security. After you configure your deployment, you can access and configure the individual components of each managed host in your deployment.

## Deployment editor requirements

Before you can use the deployment editor, ensure that it meets the minimum system requirements.

The deployment editor requires Java™ Runtime Environment (JRE). You can download Java™ 1.6 or 1.7 from the [Java™ website](http://www.java.com) (www.java.com). If you are using the Mozilla Firefox web browser, you must configure your browser to accept Java™ Network Language Protocol (JNLP) files.

Many web browsers that use the Microsoft™ Internet Explorer engine, such as Maxthon, install components that might be incompatible with the **Admin** tab. You might be required to disable any web browsers that are installed on your system.

To access the deployment editor from behind a proxy server or firewall, you must configure the appropriate proxy settings on your desktop. The software can then automatically detect the proxy settings from your browser.

To configure the proxy settings, open the Java™ configuration in your Control Pane and configure the IP address of your proxy server. For more information, see the Microsoft™ documentation.

## Deployment editor views

The deployment editor provides the different views of your deployment.



You can access the deployment editor by using the **Admin** tab. You can use the deployment editor to create your deployment, assign connections, and configure each component.

After you update your configuration settings by using the deployment editor, you must save those changes to the staging area. You must manually deploy all changes by using the **Admin** tab menu option. All deployed changes are then enforced throughout your deployment.

The deployment editor provides the following views:

## System View

Use the **System View** page to assign software component to managed hosts in your deployment. The **System View** page includes all managed hosts in your deployment. A managed host is a system in your deployment that has Extreme Security software that is installed.

By default, the **System View** page also includes the following components:

- **Host Context**, which monitors all Extreme Security components to ensure that each component is operating as expected.
- **Accumulator**, which analyzes events, reporting, writing database data, and alerting a device system module (DSM).

An accumulator is on any host that contains an Event Processor.

On the **System View** page, the left pane provides a list of managed hosts, which you can view and configure. The deployment editor polls your deployment for updates to managed hosts. If the deployment editor detects a change to a managed host in your deployment, a message is displayed notifying you of the change. For example, if you remove a managed host, a message is displayed, indicating that the assigned components to that host must be reassigned to another host.

Also, if you add a managed host to your deployment, the deployment editor displays a message that indicates that the managed host was added.

## Event View

Use the **Event View** page to create a view of your components:

- Event Processors
- Extreme Security Event Collectors
- Off-site Sources
- Off-site Targets
- Magistrate components
- Data Nodes

On the **Event View** page, the left pane provides a list of components you can add to the view. The right pane provides a view of your deployment.

## Vulnerability View

This view is only available if Extreme Networks Security Vulnerability Manager is installed on your system.

Use the **Vulnerability View** page to create a view of your Extreme Networks Security Vulnerability Manager components. You must install Extreme Networks Security Vulnerability Manager to see this view. For more information, see the *Extreme Networks Security Vulnerability Manager User Guide*

## Configuring deployment editor preferences

You can configure the deployment editor preferences to modify the zoom increments and the presence poll frequency.

- 1 Select **File > Edit Preferences**.
- 2 To configure the **Presence Poll Frequency** parameter, type how often, in milliseconds, you want the managed host to monitor your deployment for updates.
- 3 To configure the **Zoom Increment** parameter, type the increment value when the zoom option is selected.

For example, 0.1 indicates 10%.

## Building your deployment using the Deployment Editor

Use the **Deployment Editor** on the **Admin** tab to add and configure components in your Extreme Networks Security Analytics deployment. You can also use **Deployment Editor** to see visualizations of your deployment.

To add managed hosts to an existing deployment or to add Extreme Security Event Collectors, or other appliances to your deployment, use **Deployment actions** in the **System and License Management** tool on the **Admin** tab.

Before you use the deployment editor, ensure that the following conditions are met:

- Install the Java™ Runtime Environment (JRE). You can download Java™ 1.6 or 1.7 from the [Java™ website](http://www.java.com) (www.java.com).
- If you are using the Firefox browser, you must configure your browser to accept Java™ Network Language Protocol (JNLP) files.
- Plan your Extreme Security deployment, including the IP addresses and login information for all devices in your deployment.

- 1 Click the **Admin** tab and click **Deployment Editor**.
- 2 Click the **Event View** tab and add event components to the deployment.
- 3 Click the **System View** tab, and build the system.
- 4 Configure the components.
- 5 To stage your deployment, in the **Deployment Editor**, click **File > Save to Staging**.
- 6 Deploy the configuration by choosing one of the following options on the **Admin** tab in the Extreme Security Console.
  - Click **Deploy Changes**.
  - Click **Advanced > Deploy Full Configuration**.

When you deploy the full configuration, Extreme Security restarts all services. Data collection for events stops until the deployment completes.

### Related Links

Deploying managed hosts and components after installation on page 47

After installation, you can add managed hosts to your deployment. To help distribute processing, you can add Extreme Security Event Collectors, or other appliances in your deployment.

## Generating public keys for Extreme Security products

To forward normalized events in the Extreme Networks Security Analytics deployment editor, you must copy the public key file, `/root/.ssh/id_rsa.pub`, from the off-site source to the off-site target.

If the off-site source and off-site target are on separate systems, the public key is automatically generated. If the off-site source and target are both on an all-in-one system, the public key is not automatically generated. You must manually generate the public key.

To manually generate the public key, follow these steps:

- 1 Use SSH to log in to your system as the root user.
- 2 To generate the public key, type the following command:  
`opt/qradar/bin/ssh-key-generating`
- 3 Press Enter.

The public and private key pair is generated and saved in the `/root/.ssh/id_rsa` folder.

## Event view management

Use the **Event View** page to create and manage the components for your deployment.

### Building your event view

To build your Event View, do the following steps:

- 1 Add components to your view.
- 2 Connect the components.
- 3 Connect deployments.
- 4 Rename the components so each component has a unique name.

## Event views of Extreme Security components in your deployment

Use the **Event View** page to create a view of your Extreme Networks Security Analytics components, including Event Processors, Extreme Security Event Collectors, off-site sources, off-site targets, and Magistrate components.

### *Event Collector*

Collects security events from security devices, which are known as log sources, in your network.

The Event Collector normalizes the collected events and sends the information to the Event Processor.

You can connect a non-Console Event Processor to an Event Processor on the Extreme Security Console or to another Event Processor in your deployment. The accumulator gathers event information from the Event Processor.

The Event Processor on the Extreme Security Console is always connected to the Magistrate. This connection cannot be deleted.

### *Data Node*

The Data Node receives security events from associated event processors.

The Data Node stores this security data to disk.

The Data Node is always connected to Event Processor components.

### *Off-site Source*

An off-site data source that forwards normalized data to an Event Collector. You can configure an off-site source to receive data and encrypt the data before forwarding.

Later versions of Extreme Security systems can receive data from earlier versions of Extreme Security systems. However, earlier versions cannot receive data from later versions. To avoid, upgrade all receivers before you upgrade senders.

### *Off-site Target*

Indicates an off-site device that receives event data. An off-site target can receive data only from an Event Collector.

Later versions of Extreme Security systems can receive data from earlier versions of Extreme Security systems. However, earlier versions cannot receive data from later versions. To avoid, upgrade all receivers before you upgrade senders.

### *Magistrate*

You can add one Magistrate component for each deployment. The Magistrate provides views, reports, alerts, and analysis of network traffic and security events. The Magistrate processes the events by using the custom rules that are configured to create a response. If no custom rules exist, the Magistrate uses the default rule set to process the offending event.

The Magistrate prioritizes the response and assigns a magnitude value that is based on several factors, including the number of responses, severity, relevance, and credibility.

After the Magistrate establishes the magnitude, it provides multiple options for resolution.

## Adding components

When you configure your deployment, you must use the **Event View** page in the deployment editor to add your components.

You can add the following Extreme Security components to your **Event View** page:

- Event Collector
- Event Processor

- Off-site source
  - Off-site target
  - Data Node
- 1 On the **Admin** tab, click **Deployment Editor**.
  - 2 In the **Event Components** pane, select a component that you want to add to your deployment.
  - 3 Type a unique name for the component you want to add and click **Next**.

**Note**

The name can be up to 20 characters in length and might include underscores or hyphens.

- 4 From the **Select a host to assign to** list box, select a managed host, and then click **Next**.
- 5 Click **Finish**.
- 6 Repeat steps 3 - 5 for each component you want to add to your view.
- 7 From the deployment editor menu, select **File > Save to staging**.  
The deployment editor saves your changes to the staging area and automatically closes.
- 8 On the **Admin** tab menu, click **Deploy Changes**.

## Connecting components

After you add all the necessary components in your **Event View** page, you must connect them.

Use the **Event View** page to connect components together. Some restrictions are enforced. For example, you can connect an Event Collector to an Event Processor, but not a Magistrate component.

The following table describes the components that you can connect.

**Table 42: Description of supported component connections**

Source connection	Target connection	Description
Event Collector	Event Processor	<p>An Event Collector can be connected only to one Event Processor.</p> <p>A Console Event Collector can be connected only to a Console Event Collector. This connection cannot be removed.</p> <p>A non-Console Event Collector can be connected to an <code>../variables_qradar_gen.dita#ar_gen.dita#variables_general/event_processor</code> class="- topic/ph "&gt; on the same system.</p> <p>A non-Console <code>../variables_qradar_gen.dita#ar_gen.dita#variables_general/event_collector_short_name</code> class="- topic/ph "&gt; can be connected to a remote <code>../variables_qradar_gen.dita#ar_gen.dita#variables_general/event_processor</code> class="- topic/ph "&gt;, but only if the <code>../variables_qradar_gen.dita#ar_gen.dita#variables_general/event_processor</code> class="- topic/ph "&gt; does not exist on the Console.</p>
<code>../variables_qradar_gen.dita#ar_gen.dita#variables_general/event_collector_short_name</code> class="- topic/ph ">	Off-site target	The number of connections is not restricted.
Off-site source	<code>../variables_qradar_gen.dita#ar_gen.dita#variables_general/event_collector_short_name</code> class="- topic/ph ">	The number of connections is not restricted.
<code>../variables_qradar_gen.dita#ar_gen.dita#variables_general/event_processor</code> class="- topic/ph ">	<code>../variables_qradar_gen.dita#ar_gen.dita#variables_general/magistrate_shortcode</code> class="- topic/ph "> (MPC)	<p>Only one <code>../variables_qradar_gen.dita#ar_gen.dita#variables_general/event_processor</code> class="- topic/ph "&gt; can connect to a <code>../variables_qradar_gen.dita#ar_gen.dita#variables_general/magistrate_shortcode</code> class="- topic/ph "&gt;.</p>

**Table 42: Description of supported component connections (continued)**

Source connection	Target connection	Description
../ variables_qradar_gen.dita#ar_gen.dita#variables_general/ event_processor" class="- topic/ph "/>	../ variables_qradar_gen.dita#ar_gen.dita#variables_general/ event_processor" class="- topic/ph "/>	A Console ../ variables_qradar_gen.dita#ar_gen.dita#variables_general/ event_processor" class="- topic/ph "/> cannot connect to a non-Console ../ variables_qradar_gen.dita#ar_gen.dita#variables_general/ event_processor" class="- topic/ph "/>. A non-Console ../ variables_qradar_gen.dita#ar_gen.dita#variables_general/ event_processor" class="- topic/ph "/> can be connected to another Console or non- Console ../ variables_qradar_gen.dita#ar_gen.dita#variables_general/ event_processor" class="- topic/ph "/>, but not both at the same time. A non-Console ../ variables_qradar_gen.dita#ar_gen.dita#variables_general/ event_processor" class="- topic/ph "/> is connected to a Console ../ variables_qradar_gen.dita#ar_gen.dita#variables_general/ event_processor" class="- topic/ph "/> when a non-Console managed host is added.
../ variables_qradar_gen.dita#ar_gen.dita#variables_general/ data_node" class="- topic/ph "/>	../ variables_qradar_gen.dita#ar_gen.dita#variables_general/ event_processor" class="- topic/ph "/>	You can only connect a data node to an event processor. Multiple ../ variables_qradar_gen.dita#ar_gen.dita#variables_general/ data_nodes" class="- topic/ph "/> to the same event processor to create a storage cluster.

- 1 In the **Event View** page, select the component for which you want to establish a connection.
- 2 Click **Actions > Add Connection**.  
An arrow is displayed in your map. The arrow represents a connection between two components.
- 3 Drag the end of the arrow to the component you want to establish a connection to.
- 4 Click **Save**.
- 5 Repeat these steps for all remaining components that require connections.

## Forwarding normalized events

To forward normalized events, configure an off-site Event Collector in your current deployment to receive events from an associated off-site Event Collector in the receiving deployment.

You can add the following components to your **Event View** page:

- An **Off-site Source** is an off-site Event Collector from which you want to receive event data.



### Note

The off-site source must be configured with appropriate permissions to send event data to the off-site target.

- An **Off-site Target** is an off-site Event Collector to which you want to send event data.

### Example

To forward normalized event between two deployments (A and B), where deployment B wants to receive events from deployment A:

- 1 Configure deployment A with an off-site target to provide the IP address of the managed host that includes Event Collector B.
- 2 Connect Event Collector A to the off-site target.
- 3 In deployment B, configure an off-site source with the IP address of the managed host that includes Event Collector A and the port that Event Collector A is monitoring.

If you want to disconnect the off-site source, you must remove the connections from both deployments. From deployment A, remove the off-site target and in deployment B, remove the off-site source.

To enable encryption between deployments, you must enable encryption on both off-site source and target. Also, you must ensure the SSH public key for the off-site source (client) is available to the target (server) to ensure appropriate access. For example, to enable encryption between the off-site source and Event Collector B:

- 1 Create ssh keys using the `ssh-keygen -l -t rsa` command and press enter when prompted about directory and passphrase. This places the file in the `/root/.ssh` directory by default..
- 2 Copy the `id_rsa.pub` file to the `/root/.ssh` directory on the Event Collector and the source console. Rename the file to `authorized_keys`.

If you have not assigned rw owner privileges (`chmod 600 authorized_keys`) to the file and parent directory, you can use the `ssh-copy-id` command. For example, `ssh-copy-id -i hostUsername@hostIP`. The `-i` specifies that the identity file `/root/.ssh/id_rsa.pub` be used. For example, `ssh-copy-id -i root@10.100.133.80`. This command will append all entries or create an `authorized_keys` file on the target console with the right privileges. It does not check for duplicate entries. The `authorized_keys` also needs to be present on the console where other features are used. If a managed host is added to a console that is forwarding events, then an `authorized_keys` file also needs to be present in its `/root/.ssh` directory. If not, adding a managed host will fail. This is required regardless if encryption is used between the managed host and the console.

- 3 On the source console, create a `ssh_keys_created` file under `/opt/qradar/conf`. This file needs to be created so that the forwarding of events is not interrupted when other features (such as adding a managed host to one of the consoles) are combined together. Change the owner and group to **nobody** and the permission to **775** if required. `chown nobody:nobody /opt/qradar/conf/ssh_keys_created` and `chmod 775 /opt/qradar/conf/ssh_keys_created` to make sure the file can be backed up and restored properly.
- 4 Follow the off-site source and target step for 2 consoles. Program the target console first and then deploy changes. Program the source console next and then deploy changes.

If the off-site source or target is an all-in-one system, the public key is not automatically generated, therefore, you must manually generate the public key. For more information about generating public keys, see your Linux™ documentation.

If you update your Event Collector configuration or the monitoring ports, you must manually update your source and target configurations to maintain the connection between deployments.

- 1 On the **Admin** tab, click **Deployment Editor**.



- 2 In the **Event Components** pane, select **Off-site Source** or **Off-site Target**.
- 3 Type a unique name for the off-site source or off-site target. The name can be up to 20 characters in length and might include underscores or hyphens. Click **Next**.
- 4 Enter values for the parameters and click **Finish**.

The host name for the **Enter a name for the off-site host** field can contain a maximum of 20 characters and can include underscores or hyphens characters.

If you select the **Encrypt traffic from off-site source** the check box, you must also select the encryption check box on the associated off-site source and target.

- 5 Repeat for all remaining off-site sources and targets.
- 6 From the deployment editor menu, click **File > Save to staging**.
- 7 On the **Admin** tab menu, select **Advanced > Deploy Full Configuration**.

When you deploy the full configuration, Extreme Security restarts all services. Data collection for events stops until the deployment completes.

## Renaming components

You must rename a component in your view to uniquely identify components through your deployment.

- 1 In the **Event Components** pane, select the component that you want to rename.
- 2 Click **Actions > Rename Component**.
- 3 Type a new name for the component.  
The name must be alphanumeric with no special characters.
- 4 Click **OK**.

## Viewing the progress of data rebalancing

After you install a Data Node in your deployment, view the progress of data that is moving between the event processor and the Data Node. If data rebalancing is complete, you can view additional information about deployed Data Nodes.

- 1 On the Extreme Security Console, click the **Admin** tab to view the status of data nodes in your deployment at the top of the window.
- 2 Click **View** in the **Detail** column to open the **System and License Details** window.
- 3 View the progress of any data rebalancing, and the capacity of the Data Node appliance in the **Security Data Distribution** pane.

## Archiving Data Node content

When you set a Data Node appliance to **Archive** mode, no data is written to the appliance. Existing data is saved.

- 1 In the Deployment Editor, right-click the Data Node that you want to set to archive mode and click **Configure..**
- 2 Click **Archive**.

- 3 From the **Admin** tab menu, click **Deploy Changes**.
- 4 If you want to resume balancing data to a Data Node that is in archive mode, right-click **Configure > Active**.

## Saving event processor data to a Data Node appliance

Improve event processor performance by saving all data to a Data Node appliance, rather than to the event processor. If no active Data Node appliance is available in the same cluster as the event processor, the event processor saves data locally. When a Data Node appliance becomes available, it transfers as much data as possible from the event processor. Data Nodes balance data so that all Data Nodes in a cluster have the same percentage of free space.

- 1 In the Deployment Editor, right-click the event processor that has data that you want to transfer to a Data Node appliance, and click **Configure**.
- 2 Click **Active** and select **Processing-Only** from the list.
- 3 From the **Admin** tab menu, click **Deploy Changes**.

## System view management

Use the **System View** page to select which components you want to run on each managed host in your deployment.

### Overview of the System View page

Use the **System View** page to manage all managed hosts in your network.

A managed host is a component in your network that includes Extreme Security software. If you are using a Extreme Security appliance, the components for that appliance model are displayed on the **System View** page. If your Extreme Security software is installed on your own hardware, the **System View** page includes a Host Context component.

Use the **System View** page to do the following tasks:

- Add managed hosts to your deployment.
- Use NAT networks in your deployment.
- Update the managed host port configuration.
- Assign a component to a managed host.
- Configure host context.
- Configure an accumulator.

### Software compatibility requirements for Console and non-Console hosts

You cannot add, assign, or configure components on a non-Console managed host when the Extreme Security version is incompatible with the version on the Console. If a managed host was previously assigned components and is running an incompatible version, you can still view the components. However, you are not able to update or delete the components.

## Encryption

Encryption provides greater security for all traffic between managed hosts. To provide enhanced security, Extreme Security also provides integrated support for OpenSSH. When integrated with Extreme Security, OpenSSH provides secure communication between components.

Encryption occurs between managed hosts in your deployment, therefore, your deployment must consist of more than one managed host before encryption is possible. Encryption is enabled by using SSH tunnels (port forwarding) initiated from the client. A client is the system that initiates a connection in a client/server relationship. When encryption is enabled for a managed host, encryption tunnels are created for all client applications on a managed host. Encryption tunnels provide protected access to the respective servers. If you enable encryption on a non-Console managed host, encryption tunnels are automatically created for databases and other support service connections to the Console.

When you enable encryption on a managed host, the encryption SSH tunnel is created on the client host. For example, the connection between the Event Processor and Event Collector and the connection between the Event Processor and Magistrate are encrypted.



### Tip

You can right-click a component to enable encryption between components.



### Note

Enabling encryption reduces the performance of a managed host by at least 50%.

## Adding a managed host

Use the **System View** page of the deployment editor to add a managed host.

Ensure that you installed Extreme Security on the managed host.

If you want to enable Network Address Translation (NAT) for a managed host, the network must use static NAT translation. For more information, see [NAT management](#) on page 129.

If you want to add a NAT-enabled managed host to a Console that is not configured to support NAT, you must disable NAT on the Console. For more information, see [Changing the NAT status for a managed host](#) on page 130.

- 1 Click **Actions > Add a Managed Host**.
- 2 Click **Next**.
- 3 Enter values for the parameters.

Use the following table to help you configure the parameters.

**Table 43: Parameters for the managed host**

Header	Header
<b>Host is NATed</b>	Select the check box to use an existing Network Address Translation (NAT) on this managed host.
<b>Enable Encryption</b>	Select the check box to create an SSH encryption tunnel for the host.
	Select the check box to enable data compression between two managed hosts.

- If you selected the **Host is NATed** check box, configure the parameters.

**Table 44: Parameters for a NAT-enabled network**

Parameter	Description
<b>Enter public IP of the server or appliance to add</b>	The managed host uses this IP address to communicate with other managed hosts in different networks by using NAT.
<b>Select NATed network</b>	If the managed host is on the same subnet as the Console, select the Console of the NAT-enabled network . If the managed host is not on the same subnet as the Console, select the managed host of the NAT-enabled network.

- Click **Next**.
- Click **Finish**.
- Deploy your changes.

## Related Links

[NAT management](#) on page 129

Use the deployment editor to manage NAT-enabled deployments.

## Editing a managed host

Use the **System View** page of the deployment editor to edit a managed host.

If you want to enable Network Address Translation (NAT) for a managed host, the network must use static NAT translation. For more information, see [NAT management](#) on page 129.

If you want to add a NAT-enabled managed host to a Console that is not configured to support NAT, you must disable NAT on the Console. For more information, see [Changing the NAT status for a managed host](#) on page 130.

- Click the **System View** tab.
- Right-click the managed host that you want to edit and select **Edit Managed Host**.  
This option is available only when the selected component has a managed host that is running a compatible version of Extreme Security.
- Click **Next**.
- Edit the parameter values, as necessary.  
Use the following table to help you configure the parameters.

**Table 45: Parameters for the managed host**

Header	Header
<b>Host is NATed</b>	Select the check box to use an existing Network Address Translation (NAT) on this managed host.
<b>Enable Encryption</b>	Select the check box to create an SSH encryption tunnel for the host.
	Select the check box to enable data compression between two managed hosts.

- If you selected the **Host is NATed** check box, configure the parameters.


**Table 46: Parameters for a NAT-enabled network**

Parameter	Description
<b>Enter public IP of the server or appliance to add</b>	The managed host uses this IP address to communicate with other managed hosts in different networks by using NAT.
<b>Select NATed network</b>	If the managed host is on the same subnet as the Console, select the Console of the NAT-enabled network . If the managed host is not on the same subnet as the Console, select the managed host of the NAT-enabled network.

- Click **Next**.
- Click **Finish**.

## Removing a managed host

You can remove non-Console managed hosts from your deployment. You cannot remove a managed host that hosts the Extreme Security Console.

 **Tip** The **Remove host** option is available only when the selected component has a managed host that is running a compatible version of Extreme Security.

- Click the **System View** tab.
- Right-click the managed host that you want to delete and select **Remove host**.
- Click **OK**.
- On the **Admin** tab menu, click **Advanced > Deploy Full Configuration**.

When you deploy the full configuration, Extreme Security restarts all services. Data collection for events stops until the deployment completes.

## Configuring a managed host

Use the **System View** page of the deployment editor to configure a managed host.

- From the **System View** page, right-click the managed host that you want to configure and click **Configure**.
- Enter values for the parameters:  
In the **Ports to exclude** field, use a comma to separate multiple ports
- Click **Save**.

## Assigning a component to a host

Use the **System View** page to assign the Extreme Security components that you added in the **Event View** page to the managed hosts in your deployment.



### Tip

The list box displays only the managed hosts that are running a compatible version of Extreme Security.

- 1 Click the **System View** tab.
- 2 From the **Managed Host** list, select the managed host that you want to assign a Extreme Security component to.
- 3 Select the component that you want to assign to a managed host.
- 4 From the menu, select **Actions > Assign**.
- 5 From the **Select a host** list box, select the host that you want to assign to this component. Click **Next**.
- 6 Click **Finish**.

## Configuring Host Context





Use the **System View** page of the deployment editor to configure the Host Context component on a managed host.

The Host Context component monitors all Extreme Security components to make sure that each component is operating as expected.

- 1 In the deployment editor, click the **System View** tab.
- 2 Select the managed host that includes the host context you want to configure.
- 3 Select the Host Context component.
- 4 Click **Actions > Configure**.

- 5 Enter values for the parameters.

**Table 47: Host Context parameters**

Parameter	Description
<b>Warning Threshold</b>	<p>When the configured threshold of disk usage is exceeded, an email is sent to the administrator that indicates the current state of disk usage.</p> <p>The default warning threshold is 0.75. Therefore, when disk usage exceeds 75%, an email that indicates that disk usage is exceeding 75% is sent.</p> <p>If disk usage continues to increase above the configured threshold, a new email is sent after every 5% increase in usage. By default, Host Context monitors the following partitions for disk usage:</p> <ul style="list-style-type: none"> <li>• /</li> <li>• /store</li> <li>• /store/tmp</li> </ul> <hr/> <p><b>Note</b></p>  <p>Notification emails are sent from the email address that is specified in the <b>Alert Email From Address</b> parameter to the email address specified in the <b>Administrative Email Address</b> parameter. These parameters are configured on the <b>System Settings</b> window. For more information, see <a href="#">Set up Extreme Security</a> on page 62.</p>
<b>Recovery Threshold</b>	<p>When the system exceeds the shutdown threshold, disk usage must fall below the recovery threshold before processes are restarted. The default is 0.90. Therefore, processes are not restarted until disk usage is below 90%.</p> <hr/> <p><b>Note</b></p>  <p>Notification emails are sent from the email address that is specified in the <b>Alert Email From Address</b> parameter to the email address specified in the <b>Administrative Email Address</b> parameter. These parameters are configured on the <b>System Settings</b> window. For more information, see <a href="#">Set up Extreme Security</a> on page 62.</p>
<b>Shutdown Threshold</b>	<p>When the system exceeds the shutdown threshold, all processes are stopped. An email is sent to the administrator that indicates the current state of the system. The default is 0.95, therefore, when disk usage exceeds 95%, all processes stop.</p> <hr/> <p><b>Note</b></p>  <p>Notification emails are sent from the email address that is specified in the <b>Alert Email From Address</b> parameter to the email address specified in the <b>Administrative Email Address</b> parameter. These parameters are configured on the <b>System Settings</b> window.</p> <hr/> <p><b>Note</b></p>  <p>For more information, see <a href="#">Set up Extreme Security</a> on page 62.</p>
<b>Inspection Interval</b>	The frequency, in milliseconds, that you want to determine disk usage.
<b>Inspection Interval</b>	The frequency, in milliseconds, that you want to inspect SAR output.

**Table 47: Host Context parameters (continued)**

Parameter	Description
Alert Interval	The frequency, in milliseconds, that you want to be notified that the threshold was exceeded.
Time Resolution	The time, in seconds, that you want the SAR inspection to be engaged.
Inspection Interval	The frequency, in milliseconds, that you want to monitor the log files.
Monitored SYSLOG File Name	A file name for the SYSLOG file.
Alert Size	The maximum number of lines you want to monitor from the log file.

- 6 Click **Save**.

## Configuring an accumulator

Use the **System View** page of the deployment editor to configure the accumulator component on a managed host.

The accumulator component assists with data collection and anomaly detection for the Event Processor on a managed host. The accumulator component is responsible for receiving streams of events from the local Event Processor, writing database data, and contains the anomaly detection engine (ADE).

- 1 In the deployment editor, click the **System View** tab.
- 2 Select the managed host that you want to configure.
- 3 Select the accumulator component.
- 4 Click **Actions > Configure**.
- 5 Configure the parameters.

**Table 48: Accumulator parameters**

Parameter	Description
Central Accumulator	Specifies whether the current component is a central accumulator. A central accumulator exists only on a Console system.
Anomaly Detection Engine	ADE is responsible for analyzing network data and forwarding the data to the rule system for resolution. For the central accumulator, type the address and port using the following syntax: <code>&lt;Console&gt;:&lt;port&gt;</code> For a non-central accumulator, type the address and port using the following syntax: <code>&lt;non-Console IP Address&gt;:&lt;port&gt;</code>
Alerts DSM Address	The device system module (DSM) address that is used to forwarding alerts from the accumulator. Use the following syntax: <code>&lt;DSM_IP address&gt;:&lt;DSM port number&gt;</code> .

- 6 Click **Save**.



## NAT management

Use the deployment editor to manage NAT-enabled deployments.

Network address translation (NAT) translates an IP address in one network to a different IP address in another network. NAT provides increased security for your deployment since requests are managed through the translation process and hides internal IP addresses.

You can add a non-NAT-enabled managed host by using inbound NAT for a public IP address. You can also use a dynamic IP address for outbound NAT. However, both must be on the same switch as the Console or managed host. You must configure the managed host to use the same IP address for the public and private IP addresses.

When you add or edit a managed host, you can enable NAT for that managed host. You can also use the deployment editor to manage your NAT-enabled networks.

### Adding a NAT-enabled network to Extreme Security

Use the deployment editor to add a NAT-enabled network to your Extreme Security deployment.

Ensure that you set up your NAT-enabled networks by using static NAT translation. This setup ensures that communications between managed hosts that exist within different NAT-enabled networks.

- 1 In the deployment editor, click the **NATed Networks** icon.
- 2 Click **Add**.
- 3 Type a name for a network you want to use for NAT.
- 4 Click **OK**.

The **Manage NATed Networks** window is displayed, including the added NAT-enabled network.

- 5 Click **OK**.
- 6 Click **Yes**.

### Editing a NAT-enabled network

Using the deployment editor, you can edit a NAT-enabled network.

- 1 In the deployment editor, click the **NATed Networks** icon.
- 2 Select the NAT-enabled network that you want to edit, and click **Edit**.
- 3 Type a new name for of the NAT-enabled network and click **OK**.

The **Manage NATed Networks** window shows the updated NAT-enabled networks.

- 4 Click **OK**.
- 5 Click **Yes**.

### Deleting a NAT-enabled network from Extreme Security

Use the deployment editor to delete a NAT-enabled network from your deployment:

- 1 In the deployment editor, click the **NATed Networks** icon.
- 2 Select the NAT-enabled network you want to delete.

- 3 Click **Delete**.
- 4 Click **OK**.
- 5 Click **Yes**.

## Changing the NAT status for a managed host

Use the deployment editor to change the NAT status of a managed host in your deployment.

If you want to enable NAT for a managed host, the NAT-enabled network must be using static NAT translation.

To change your NAT status for a managed host, make sure you update the managed host configuration within Extreme Security before you update the device. Updating the configuration first prevents the host from becoming unreachable and you can deploy changes to that host.

- 1 In the deployment editor, click the **System View** tab.
- 2 Right-click the managed host that you want to edit and select **Edit Managed Host**.
- 3 Click **Next**.
- 4 Choose one of the following options:
  - If you want to enable NAT for the managed host, select the **Host is NATed** check box and click **Next**.
  - If you want to disable NAT for the managed host, clear the **Host is NATed** check box.



### Note

When you change the NAT status for an existing managed host, error messages might be displayed. Ignore these error messages.

- 5 If you enabled NAT, select a NAT-enabled network, and enter values for the parameters:

**Table 49: Parameters for a NAT-enabled network**

Parameter	Description
Change public IP of the server or appliance to add	The managed host uses this IP address to communicate with another managed host that belongs to a different network by using NAT.
Select NATed network	Update the NAT-enabled network configuration.
Manage NATs List -	Network address translation (NAT) translates an IP address in one network to a different IP address in another network. NAT provides increased security for your deployment since requests are managed through the translation process and hides internal IP addresses. For more information, see <a href="#">NAT management</a> on page 129.

- 6 Click **Next**.
- 7 Click **Finish**.
- 8 Update the configuration for the device (firewall) to which the managed host is communicating.
- 9 On the **Admin** tab menu, click **Advanced** > **Deploy Full Configuration**.

When you deploy the full configuration, Extreme Security restarts all services. Data collection for events stops until the deployment completes.

## Component configuration

Use the deployment editor to configure each component in your deployment.

### Configuring an Event Collector

Use the deployment editor to configure an Event Collector.

- 1 From either the **Event View** or **System View** page, select the Event Collector that you want to configure.
- 2 Click **Actions > Configure**.
- 3 Enter values for the following parameters:

Parameter	Description
<b>Destination Event Processor</b>	Specifies the Event Processor component that is connected to this Event Collector. The connection is displayed in the following format: <b>&lt;Host IP Address&gt; : &lt;Port&gt;</b> .
<b>Event Forwarding Listen Port</b>	The Event Collector event forwarding port.

- 4 On the toolbar, click **Advanced** to display the advanced parameters.
- 5 Configure the advanced parameters, as necessary.

**Table 50: Event Collector advanced parameters**

Parameter	Description
<b>Primary Collector</b>	<b>True</b> specifies that the Event Collector is on a Console system. <b>False</b> specifies that the Event Collector is on a non-Console system.
<b>Autodetection Enabled</b>	<b>Yes</b> enables the Event Collector to automatically analyze and accept traffic from previously unknown log sources. The appropriate firewall ports are opened to enable Autodetection to receive events. This option is the default. <b>No</b> prevents the Event Collector from automatically analyzing and accepting traffic from previously unknown log sources. For more information, see the <i>Extreme Networks Security Managing Log Sources Guide</i> .
<b>Forward Events Already Seen</b>	<b>True</b> enables the Event Collector to forward events that was detected on the system. <b>False</b> prevents the Event Collector from forwarding events that was detected on the system. This option prevents event-looping on your system.

- 6 Click **Save**.
- 7 Repeat for all Extreme Security Event Collectors in your deployment you want to configure.

#### Related Links

[Event views of Extreme Security components in your deployment](#) on page 115

### Configuring an Event Processor

Use the deployment editor to configure an Event Processor.

- 1 From either the **Event View** or **System View** page, select the Event Processor that you want to configure.

- 2 Click **Actions > Configure**.
- 3 Enter values for the parameters:

**Table 51: Parameter values for the Event Processor**

Parameter	Description
Event Collector Connections Listen Port	The port that the Event Processor monitors for incoming Event Collector connections. The default value is port 32005.
Event Processor Connections Listen Port	The port that the Event Processor monitors for incoming Event Processor connections. The default value is port 32007.

- 4 On the toolbar, click **Advanced** to display the advanced parameters.
- 5 Enter values for the parameters, as necessary.

**Table 52: Event Processor advanced parameters**

Parameter	Description
Test Rules	<p>The <b>test rules</b> list is available only for non-Console Event Processors. If a rule is configured to test locally, the <b>Globally</b> option does not override the rule setting. If you select <b>Locally</b>, rules are tested on the Event Processor and not shared with the system.</p> <p>If you select <b>Globally</b>, individual rules for every Event Processor are shared and tested system wide. Each rule can be toggled to <b>Global</b> for detection by any Event Processor on the system.</p> <p>For example, you can create a rule to alert you when there are five failed login attempts within 5 minutes. When the Event Processor that contains the local rule observes five failed login attempts, the rule generates a response. If the rule in the example is set to Global, when five failed login attempts within 5 minutes are detected on any Event Processor, the rule generates a response. When rules are shared globally, the rule can detect when one failed login attempt comes from five event processors.</p> <p>Testing rules globally is the default for non-Console Event Processor with each rule on the Event Processor set to test locally.</p>
Overflow Event Routing Threshold	Type the events per second threshold that the Event Processor can manage. Events over this threshold are placed in the cache.
Events database path	Type the location that you want to store events. The default is <code>/store/ariel/events</code> .
Payloads database length	The location that you want to store payload information. The default is <code>/store/ariel/payloads</code> .

- 6 Click **Save**.
- 7 Repeat for all Event Processors in your deployment you want to configure.

## Related Links

[Event views of Extreme Security components in your deployment](#) on page 115

## Configuring the Magistrate

Use the deployment editor to configure a Magistrate component.

- 1 From either the **Event View** or **System View** page, select the Magistrate that you want to configure.

- 2 Click **Actions > Configure**.
- 3 On the toolbar, click **Advanced** to display the advanced parameters.
- 4 In the **Overflow Routing Threshold** field, type the events per second threshold that the Magistrate can manage events.  
Events over this threshold are placed in the cache.  
  
The default is 20,000.
- 5 Click **Save**.

#### Related Links

[Event views of Extreme Security components in your deployment](#) on page 115

## Configuring an off-site source

Use the deployment editor to configure an off-site source.

To prevent connection errors, when you configure off-site source and target components, deploy the Extreme Security Console with the off-site source first. Then deploy the Extreme Security Console with the off-site target.

- 1 From either the **Event View** or **System View** page, select the Event Collector that you want to configure.
- 2 Click **Actions > Configure**.
- 3 Enter the parameter values.

Parameter	Description
<b>Receive Events</b>	<b>True</b> enables the system to receive events from the off-site source host. <b>False</b> prevents the system from receiving events from the off-site source host.

- 4 Click **Save**.
- 5 Repeat for all off-site sources in your deployment you want to configure.

#### Related Links

[Event views of Extreme Security components in your deployment](#) on page 115

## Configuring an off-site target

Use the deployment editor to configure an off-site target.

To prevent connection errors, when you configure off-site source and target components, deploy the Extreme Security Console with the off-site source first. Then, deploy the Extreme Security Console with the off-site target.

- 1 From either the **Event View** or **System View** page, select the Event Collector that you want to configure.
- 2 Click **Actions > Configure**.

- 3 Enter values for the parameters:

Parameter	Description
Event Collector Listen Port	The Event Collector listen port for receiving event data. The default port for events is 32004.

- 4 Click **Save**.

#### Related Links

[Event views of Extreme Security components in your deployment](#) on page 115

# 11 Domain segmentation

**Overlapping IP addresses**

**Domain definition and tagging**

**Creating domains**

**Domain privileges that are derived from security profiles**

**Domain-specific rules**

**Example: Domain privilege assignments based on custom properties**

Segmenting your network into different domains helps to ensure that relevant information is available only to those users that need it.

You can create security profiles to limit the information that is available to a group of users within that domain. Security profiles provide authorized users access to only the information that is required to complete their daily tasks. You modify only the security profile of the affected users, and not each user individually.

You can also use domains to manage overlapping IP address ranges. This method is helpful when you are using a shared Extreme Networks Security Analytics infrastructure to collect data from multiple networks. By creating domains that represent a particular address space on the network, multiple devices that are in separate domains can have the same IP address and still be treated as separate devices.

## Overlapping IP addresses

An overlapping IP address is an IP address that is assigned to more than one device or logical unit, such as an event source type, on a network. Overlapping IP address ranges can cause significant problems for companies that merge networks after corporate acquisitions, or for Managed Security Service Providers (MSSPs) who are bringing on new clients.

Extreme Networks Security Analytics must be able to differentiate events that come from different devices and that have the same IP address. If the same IP address is assigned to more than one event source, you can create domains to distinguish them.

For example, let's look at a situation where Company A acquires Company B and wants to use a shared instance of Extreme Security to monitor the new company's assets. The acquisition has a similar network structure that results in the same IP address being used for different log sources in each company. Log sources that have the same IP address cause problems with correlation, reporting, searching, and asset profiling.

To distinguish the origin of the events that come in to Extreme Security from the log source, you can create two domains and assign each log source to a different domain. If required, you can also assign each event collector to the same domain as the log source that sends events to them.

To view the incoming events by domain, create a search and include the domain information in the search results.

## Domain definition and tagging

Domains are defined based on input sources. When events come into , the domain definitions are evaluated and the events are tagged with the domain information.

### Specifying domains for events

These are the ways to specify domains for events:

<b>Event collectors</b>	<p>If an event collector is dedicated to a specific network segment or IP address range, you can flag that entire event collector as part of that domain.</p> <p>All log sources that arrive at that event collector belong to the domain; therefore, any new auto-detected log sources are automatically added to the domain.</p>
<b>Log sources</b>	<p>You can configure specific log sources to belong to a domain.</p> <p>This method of tagging domains is an option for deployments in which an event collector can receive events from multiple domains.</p>
<b>Log source groups</b>	<p>You can assign log source groups to a specific domain. This option allows broader control over the log source configuration.</p> <p>Any new log sources that are added to the log source group automatically get the domain tagging that is associated with the log source group.</p>
<b>Custom properties</b>	<p>You can apply custom properties to the log messages that come from a log source.</p> <p>To determine which domain that specific log messages belong to, the value of the custom property is looked up against a user-defined table.</p> <p>This option is used for multi-address-range or multi-tenant log sources, such as file servers and document repositories.</p>

### Specifying domains for scan results

You can also assign vulnerability scanners to a specific domain so that scan results are properly flagged as belonging to that domain. A domain definition can consist of all input sources.

For information about assigning your network to pre-configured domains, see [Network hierarchy](#) on page 62.

### Precedence order for evaluating domain criteria

When events come into the system, the domain criteria is evaluated based on the granularity of the domain definition.

If the domain definition is based on an event, the incoming event is first checked for any custom properties that are mapped to the domain definition. If the result of a regular expression that is defined in a custom property does not match a domain mapping, the event is automatically assigned to the default domain.



If the event does not match the domain definition for custom properties, the following order of precedence is applied:

- 1 log source
- 2 log source group
- 3 event collector

If a scanner has an associated domain, all assets that are discovered by the scanner are automatically assigned to the same domain as the scanner.

## Forwarding data to another system

Domain information is removed when data is forwarded to another system. Events that contain domain information are automatically assigned to the default domain on the receiving system. To identify which events are assigned to the default domain, you can create a custom search on the receiving system. You might want to reassign these events to a user-defined domain.

## Creating domains

Use the **Domain Management** window to create domains based on Extreme Networks Security Analytics input sources.

Use the following guidelines when you create domains:

- Everything that is not assigned to a user-defined domain is automatically assigned to the default domain. Users who have limited domain access should not have administrative privileges because this privilege grants unlimited access to all domains.
- You can map the same custom property to two different domains, however the capture result must be different for each one.
- You cannot assign a log source, log source group, or event collector to two different domains. When a log source group is assigned to a domain, each of the mapped attributes is visible in the **Domain Management** window.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration**.
- 3 Click **Domain Management**.
- 4 To add a domain, click **Add** and type a unique name and description for the domain.



### Tip

You can check for unique names by typing the name in the **Input domain name** search box.

- 5 Depending on the domain criteria to be defined, click the appropriate tab.
  - To define the domain based on a custom property, log source group, log source, or event collector, click the **Events** tab.
  - To define the domain based on a scanner, including Extreme Networks Security Vulnerability Manager scanners, click the **Scanners** tab.

- 6 To assign a custom property to a domain, in the **Capture Result** box, type the text that matches the result of the regular expression (regex) filter.



#### Note

You must select the **Optimize parsing for rules, reports, and searches** check box in the **Custom Event Properties** window to parse and store the custom event property. Domain segmentation will not occur if this option is not checked.

- 7 From the list, select the domain criteria and click **Add**.
- 8 After you add the source items to the domain, click **Create**.

**Create security profiles** to define which users have access to the domains. After you create the first domain in your environment, you must update the security profiles for all non-administrative users to specify the domain assignment. In domain-aware environments, non-administrative users whose security profile does not specify a domain assignment will not see any log activity or network activity.

You can also use the Network Hierarchy tool to assign your network to pre-configured domains. For more information, see [Network hierarchy](#) on page 62.

## Domain privileges that are derived from security profiles

You can use security profiles to grant domain privileges and ensure that domain restrictions are respected throughout the entire Extreme Networks Security Analytics system. Security profiles also make it easier to manage privileges for a large group of users when your business requirements suddenly change.

Users can see only data within the domain boundaries that are set up for the security profiles that are assigned to them. Security profiles include domains as one of the first criteria that is evaluated to restrict access to the system. When a domain is assigned to a security profile, it takes priority over other security permissions. After domain restrictions are evaluated, individual security profiles are assessed to determine network and log permissions for that particular profile.

For example, a user is given privileges to Domain\_2 and access to network 10.0.0.0/8. That user can see only events that come from Domain\_2 and contain an address from the 10.0.0.0/8 network.

As a Extreme Security administrator, you can see all domains and you can assign domains to non-administrative users. Do not assign administrative privileges to users whom you want to limit to a particular domain.

When you assign domains to a security profile, you can grant access to the following types of domains:

<b>User-defined domains</b>	You can create domains that are based on input sources by using the Domain Management tool. For more information, see <i>Creating domains</i> . <a href="#">Creating domains</a> .
<b>Default domain</b>	Everything that is not assigned to a user-defined domain is automatically assigned to the default domain. The default domain contains system-wide events.



#### Note

Users who have access to the default domain can see system-wide events without restriction. Ensure that this access is acceptable before you assign default domain access to users. All administrators have access to the default domain.

Any log source that gets auto-discovered on a shared event collector (one that is not explicitly assigned to a domain), is auto-discovered on the default domain. These log sources require manual intervention. To identify these log sources, you must periodically run a search in the default domain that is grouped by log source.

**All domains** Users who are assigned to a security profile that has access to **All Domains** can see all active domains within the system, the default domain, and any domains that were previously deleted across the entire system. They can also see all domains that are created in the future.

If you delete a domain, it cannot be assigned to a security profile. If the user has the **All domains** assignment, or if the domain was assigned to the user before it was deleted, the deleted domain is returned in historical search results for events. You can't filter by deleted domains when you run a search.

Administrative users can see which domains are assigned to the security profiles on the **Summary** tab in the **Domain Management** window.

## Rule modifications in domain-aware environments

Rules can be viewed, modified, or disabled by any user who has both the **Maintain Custom Rules** and **View Custom Rules** permissions, regardless of which domain that user belongs to.

To prevent domain users from being able to modify rules in other domains, edit the user role and remove the **Maintain Custom Rules** and **View Custom Rules** permissions. To provide domain users the ability to modify rules only within a specific domain, create a trusted user role for each domain and grant the **Maintain Custom Rules** and **View Custom Rules** permissions.

## Domain-aware searches

You can use domains as search criteria in custom searches. Your security profile controls which domains you can search against.

System-wide events and events that are not assigned to a user-defined domain are automatically assigned to the default domain. Administrators, or users who have a security profile that provides access to the default domain, can create a custom search to see all events that are not assigned to a user-defined domain.

---

## Domain-specific rules

A rule can work in the context of a single domain or in the context of all domains. Domain-aware rules provide the option of including the **And Domain Is** test.

You can restrict a 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.

Rules that work in the context of all domains are referred to as system-wide rules. To create a system-wide rule that tests conditions across the entire system, select **Any Domain** in the domain list for the **And Domain Is** test.

**Single-domain rule** If the rule is a stateful rule, the states are maintained separately for each domain. The rule is triggered separately for each domain.

**System-wide rule** If the rule is a stateful rule, a single state is maintained for the whole system and domain tags are ignored.

The following table provides examples of domain-aware rules. The examples use a system that has three domains that are defined: Domain\_A, Domain\_B, and Domain\_C.

The rule examples in the following table may not be applicable in your environment. For example, rules that use flows and offenses are not applicable in .

This two-column table shows examples of domain-aware rules and the behavior of the rule when it fires.

**Table 53: Domain-aware rules**

Domain text	Explanation	Rule response
domain is one of: Domain_A	Looks only at events that are tagged with Domain_A and ignores rules that are tagged with other domains.	Creates or contributes to an offense that is tagged with Domain_A.
domain is one of: Domain_A and a stateful test that is defined as when HTTP flow is detected 10 times within 1 minute	Looks only at events that are tagged with Domain_A and ignores rules that are tagged with other domains.	Creates or contributes to an offense that is tagged with Domain_A. A single state, an HTTP flow counter, gets maintained for Domain_A.
domain is one of: Domain_A, Domain_B	Looks only at events that are tagged with Domain_A and Domain_B and ignores events that are tagged with Domain_C. This rule behaves as two independent instances of a single domain rule, and creates separate offenses for different domains.	For data that is tagged with Domain_A, it creates or contributes to a single domain offense that is tagged with Domain_A. For data that is tagged with Domain_B, it creates or contributes to a single domain offense that is tagged with Domain_B.
domain is one of: Domain_A, Domain_B and a stateful test that is defined as when HTTP flow is detected 10 times within 1 minute	Looks only at events that are tagged with Domain_A and Domain_B and ignores events that are tagged with Domain_C. This rule behaves as two independent instances of a single domain rule, and maintains two separate states (HTTP flow counters) for two different domains.	When the rule detects 10 HTTP flows that are tagged with Domain_A within a minute, it creates or contributes to an offense that is tagged with Domain_A. When the rule detects 10 HTTP flows that are tagged with Domain_B within a minute, it creates or contributes to an offense that is tagged with Domain_B.
No domain test defined	Looks at events that are tagged with all domains and creates or contributes to offenses on a per-domain basis.	Each independent domain has offenses that are generated for it, but offenses do not contain contributions from other domains.
A rule has a stateful test that is defined as when HTTP flow is detected 10 times within 1 minute and no domain test is defined	Looks at events that are tagged with Domain_A, Domain_B, or Domain_C.	Maintains separate states and creates separate offenses for each domain.

**Table 53: Domain-aware rules (continued)**

Domain text	Explanation	Rule response
<b>domain is one of: Any Domain</b>	Looks at all events, regardless of which domain it is tagged with.	Creates or contributes to a single system-wide offense that is tagged with <b>Any Domain</b> .
<b>domain is one of: Any Domain</b> and a stateful test that is defined as <b>when HTTP flow is detected 10 times within 1 minute</b>	Looks at all events, regardless of which domain it is tagged with, and it maintains a single state for all domains.	Creates or contributes to a single system-wide offense that is tagged with <b>Any Domain</b> . For example, if it detects 3 events that are tagged with <b>Domain_A</b> , 3 events that are tagged with <b>Domain_B</b> , and 4 events that are tagged with <b>Domain_C</b> within 1 minute, it creates an offense because it detected 10 events in total.
<b>domain is one of: Any Domain, Domain_A</b>	Works the same as a rule that has <b>domain is one of: Any Domain</b> .	When the domain test includes <b>Any Domain</b> , any single domains that are listed are ignored.

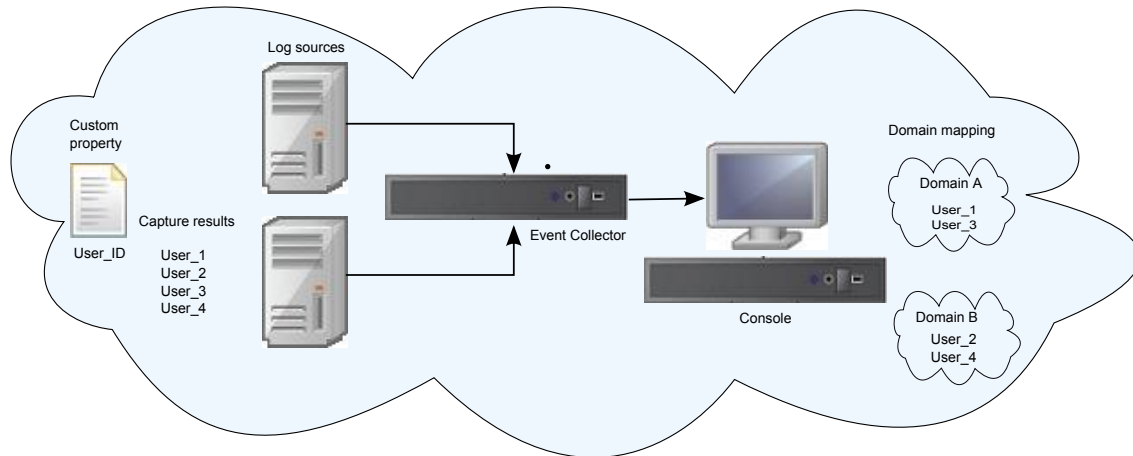
## Example: Domain privilege assignments based on custom properties

If your log files contain information that you want to use in a domain definition, you can expose the information as a custom event property.

You assign a custom property to a domain based on the capture result. You can assign the same custom property to multiple domains, but the capture results must be different.

For example, a custom event property, such as `userID`, might evaluate to a single user or a list of users. Each user can belong to only one domain.

In the following diagram, the log sources contain user identification information that is exposed as a custom property, `userID`. The capture results return a list of four users, and each user is assigned to only one domain. In this case, two users are assigned to Domain A and two users are assigned to Domain B.



**Figure 1: Assigning domains by using custom event property**

If the capture results return a user that is not assigned to a specific user-defined domain, that user is automatically assigned to the default domain. Default domain assignments require manual intervention. Perform periodic searches to ensure that all entities in the default domain are correctly assigned.

#### Note



Before you use a custom property in a domain definition, ensure that **Optimize parsing for rules, reports, and searches** is checked on the **Custom Event Properties** window. This option ensures that the custom event property is parsed and stored when Extreme Security receives the event for the first time. Domain segmentation will not occur if this option is not checked.

# 12 Asset growth deviations

## System notifications for asset growth deviations

### Prevention of asset growth deviations

#### Deleting invalid assets

#### Deleting blacklist entries

#### Modifying asset blacklists and whitelists

Extreme Networks Security Log Manager only tracks asset data if Extreme Networks Security Vulnerability Manager is installed.

Sometimes, asset data sources produce updates that Extreme Networks Security Analytics cannot handle properly without manual remediation.

Depending on the cause of the abnormal asset growth, you can either fix the asset data source that is causing the problem or you can block asset updates that come from that data source.

*Asset growth deviations* occur when the number of asset updates for a single device grows beyond the limit that is set by the retention threshold for a specific type of the identity information. Proper handling of asset growth deviations is critical to maintaining an accurate asset model.

At the root of every asset growth deviation is an asset data source whose data is untrustworthy for updating the asset model. When a potential asset growth deviation is identified, you must look at the source of the information to determine whether there is a reasonable explanation for the asset to accumulate large amounts of identity data.

Whether you fix the source of the problem or block the asset updates, you must clean up the asset database by removing the invalid asset data and the asset blacklist entries.

## 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.

## 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.qllabs.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

[Stale asset data](#) on page 146

Stale asset data can be problematic when the rate at which new asset records are created exceeds the rate at which stale asset data is removed. Controlling and managing asset retention thresholds is the key to addressing asset growth deviations that are caused by stale asset data.



## 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

[Advanced tuning of asset reconciliation exclusion rules](#) on page 151

You can tune the Asset Reconciliation Exclusion rules to refine the definition of deviating asset growth in one or more of the rules.

[Modifying asset blacklists and whitelists](#) on page 154

The asset blacklists and whitelists are reference sets. You can view and modify the asset blacklist and whitelist data using the **Reference Set Management** tool in the Extreme Security Console.

---

## Prevention of asset growth deviations

After you confirm that the reported asset growth is legitimate, there are several ways to prevent Extreme Networks Security Analytics from triggering growth deviation messages for that asset.

Use the following list to help you decide how to prevent asset growth deviations:

- Understand how Extreme Security handles stale asset data.
- Tune the asset profiler retention settings to limit the length of time that asset data is retained.
- Tune the number of IP addresses allowed for a single asset
- Create identity exclusion searches to exclude certain events from providing asset updates.
- Tune the Asset Reconciliation Exclusion rules to refine the definition of deviating asset growth.
- Create asset whitelists to prevent data from reappearing on the asset blacklists.
- Modify the entries on the asset blacklists and asset whitelists.
- Ensure that your DSMs are up to date. Extreme Security provides a weekly automatic update that might contain DSM updates and corrections to parsing issues.

Asset growth can be caused by large volumes of asset data that changes legitimately such as these situations:

- A mobile device that travels from office-to-office frequently and is assigned a new IP address whenever it logs in.
- A device that connects to a public wifi with short IP addresses leases, such as at a university campus, might collect large volumes of asset data over a semester.

Extreme Security might mistakenly report this activity as an asset growth deviation.

#### Related Links

[Automatic updates](#) on page 65

You can automatically or manually update your configuration files to ensure that your configuration files contain the latest network security information.

## Stale asset data

Stale asset data can be problematic when the rate at which new asset records are created exceeds the rate at which stale asset data is removed. Controlling and managing asset retention thresholds is the key to addressing asset growth deviations that are caused by stale asset data.

*Stale asset data* is historical asset data that is not actively or passively observed within a specific time. Stale asset data is deleted when it exceeds the configured retention period.

The historical records become active again if they are observed by Extreme Security passively, through events, or actively, through port and vulnerability scanners.

Preventing asset growth deviations requires finding the right balance between the number of IP addresses allowed for a single asset and the length of time that Extreme Security retains the asset data. You must consider the performance and manageability trade-offs before you configure Extreme Security to accommodate high levels of asset data retention. While longer retention periods and higher per-asset thresholds might appear desirable all the time, a better approach is to determine a baseline configuration that is acceptable for your environment and test that configuration. Then, you can increase the retention thresholds in small increments until the right balance is achieved.

#### Related Links

[Tuning the Asset Profiler retention settings](#) on page 148

[Tuning the number of IP addresses allowed for a single asset](#) on page 149

## 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 54: 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.

### Related Links

[Asset whitelists](#) on page 147

## Asset whitelists

You can use asset whitelists to keep Extreme Networks Security Analytics asset data from inadvertently reappearing in the asset blacklists.

An *asset whitelist* is a collection of asset data that overrides the asset reconciliation engine logic about which data is added to an asset blacklist. When the system identifies a blacklist match, it checks the whitelist to see whether the value exists. If the asset update matches data that is on the whitelist, the change is reconciled and the asset is updated. Whitelisted asset data is applied globally for all domains.

### *Example of a whitelist use case*

The whitelist is helpful if you have asset data that continues to show up in the blacklists when it is a valid asset update. For example, you might have a round robin DNS load balancer that is configured to rotate across a set of five IP addresses. The Asset Reconciliation Exclusion rules might determine that the multiple IP addresses associated with the same DNS host name are indicative of an asset growth deviation, and the system might add the DNS load balancer to the blacklist. To resolve this problem, you can add the DNS host name to the Asset Reconciliation DNS Whitelist.

### *Mass entries to the asset whitelist*

An accurate asset database makes it easier to connect offenses that are triggered in your system to physical or virtual assets in your network. Ignoring asset deviations by adding mass entries to the asset

whitelist is not helpful in building an accurate asset database. Instead of adding mass whitelist entries, review the asset blacklist to determine what is contributing to the deviating asset growth and then determine how to fix it.

### *Types of asset whitelists*

Each type of identity data is kept in a separate whitelist. The following table shows the reference collection name and type for each type of identity asset data.

**Table 55: Reference collection name for asset whitelist data**

Type of data	Reference collection name	Reference collection type
IP addresses	Asset Reconciliation IPv4 Whitelist	Reference Set [Set Type: IP]
DNS host names	Asset Reconciliation DNS Whitelist	Reference Set [Set Type: ALNIC*]
NetBIOS host names	Asset Reconciliation NetBIOS Whitelist	Reference Set [Set Type: ALNIC*]
MAC addresses	Asset Reconciliation MAC Whitelist	Reference Set [Set Type: ALNIC*]

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

### Related Links

[Asset blacklists](#) on page 147

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.

## Tuning the Asset Profiler retention settings

Extreme Networks Security Analytics uses the asset retention settings to manage the size of the asset profiles.

The default retention period for most asset data is 120 days after the last time it was either passively or actively observed in Extreme Security. User names are retained for 30 days.

Asset data that is added manually by Extreme Security users does not usually contribute to asset growth deviations. By default, this data is retained forever. For all other types of asset data, the **Retain Forever** flag is suggested only for static environments.

You can adjust the retention time based on the type of asset identity data that is in the event. For example, if multiple IP addresses are merging under one asset, you can change the Asset IP Retention period from 120 days to a lower value.

When you change the asset retention period for a specific type of asset data, the new retention period is applied to all asset data in Extreme Security. Existing asset data that already exceeds the new threshold is removed when the deployment is complete. To ensure that you can always identify named hosts even when the asset data is beyond the retention period, the asset retention cleanup process does not remove the last known host name value for an asset.

Before you determine how many days that you want to retain the asset data, understand the following characteristics about longer retention periods:

- provides a better historical view of your assets.
- creates larger data volumes per asset in the asset database.
- increases the probability that stale data will contribute to asset growth deviation messages.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration**.
- 3 Click **Asset Profiler Configuration**.
- 4 Click **Asset Profiler Retention Configuration**.
- 5 Adjust the retention values and click **Save**.
- 6 Deploy the changes into your environment for the updates to take effect.

#### Related Links

[Tuning the number of IP addresses allowed for a single asset](#) on page 149

## Tuning the number of IP addresses allowed for a single asset

Extreme Networks Security Analytics monitors the number of IP addresses that a single asset accumulates over time.

By default, Extreme Security generates a system message when a single asset accumulates more than 75 IP addresses. If you expect assets to accumulate more than 75 IP addresses, you can tune the **Number of IPs Allowed for a Single Asset** value to avoid future system messages.

Setting the limit for the number of IP addresses too high prevents Extreme Security from detecting asset growth deviations before they have a negative impact on the rest of the deployment. Setting the limit too low increases the number of asset growth deviations that are reported.

You can use the following guideline when you tune the **Number of IPs Allowed for a Single Asset** setting for the first time.

Number of IP addresses that are allowed for a single asset = (*<retention time (days)>* × *<estimated IP addresses per day>*) + *<buffer number of IP addresses>*

Where

- *<estimated IP addresses per day>* is the number of IP addresses that a single asset might accumulate in one day under normal conditions
- *<retention time (days)>* is the preferred amount of time to retain the asset IP addresses

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration**.
- 3 Click **Asset Profiler Configuration**.
- 4 Click **Asset Profiler Retention Configuration**.
- 5 Adjust the configuration values and click **Save**.
- 6 Deploy the changes into your environment for the updates to take effect.

#### Related Links

[Tuning the Asset Profiler retention settings](#) on page 148

## Identity exclusion searches

Identity exclusion searches can be used to manage single assets that accumulate large volumes of similar identity information for known, valid reasons.

For example, log sources can provide large volumes of asset identity information to the asset database. They provide Extreme Networks Security Analytics with near real-time changes to asset information and they can keep your asset database current. But log sources are most often the source of asset growth deviations and other asset-related anomalies.

When a log source sends incorrect asset data to Extreme Security, try to fix the log source so that the data it sends is usable by the asset database. If the log source cannot be fixed, you can build an identity exclusion search that blocks the asset information from entering the asset database.

You can also use an identity exclusion search where **Identity\_Username+Is Any Of + Anonymous Logon** to ensure that you are not updating assets that are related to service accounts or automated services.

### *Differences between identity exclusion searches and blacklists*

While identity exclusion searches appear to have similar functionality to asset blacklists, there are significant differences.

Blacklists can specify only raw asset data, such as MAC addresses and host names, that is to be excluded. Identity exclusion searches filter out asset data based on search fields like log source, category, and event name.

Blacklists do not account for the type of data source that is providing the data, whereas identity exclusion searches can be applied to events only. Identity exclusion searches can block asset updates based on common event search fields, such as event type, event name, category, and log source.

### *Creating identity exclusion searches*

To exclude certain events from providing asset data to the asset database, you can create a Extreme Networks Security Analytics identity exclusion search.

The filters that you create for the search must match events that you want to exclude, not the events that you want to keep.

You might find it helpful to run the search against events that are already in the system. However, when you save the search, you must select **Real Time (streaming)** in the **Timespan** options. If you do not choose this setting, the search will not match any results when it runs against the live stream of events that are coming into Extreme Security.

When you update the saved identity exclusion search without changing the name, the identity exclusion list that is used by the Asset Profiler is updated. For example, you might edit the search to add more filtering of the asset data that you want to exclude. The new values are included and the asset exclusion starts immediately after the search is saved.

- 1 On the **Log Activity** tab, click **Search > New Search**.

- 2 Create the search by adding search criteria and filters to match the events that you want to exclude from asset updates.
- 3 In the **Time Range** box, select **Real Time (streaming)** and then click **Filter** to run the search.
- 4 On the search results screen, click **Save Criteria** and provide the information for the saved search.  
You can assign the saved search to a search group. An Identity Exclusion search group exists in the **Authentication, Identity and User Activity** folder.

Ensure that **Real Time (streaming)** is selected in the **Timespan** options.

- 5 Click **OK** to save the search.
- 6 Click the **Admin** tab, and click **Asset Profiler Configuration**.
- 7 Click **Manage Identity Exclusion** at the bottom of the screen.
- 8 Select the identity exclusion search that you created from the list of searches on the left and click the add icon (>).

If you can't find the search, type the first few letters into the filter at the top of the list.

- 9 Click **Save**.
- 10 Deploy the changes into your environment for the updates to take effect.

## Related Links

[Deploying changes](#) on page 14

You can update your configuration settings from the **Admin** tab. Your changes are saved to a staging area where they are stored until you manually deploy the changes.

## Advanced tuning of asset reconciliation exclusion rules

You can tune the Asset Reconciliation Exclusion rules to refine the definition of deviating asset growth in one or more of the rules.

For example, consider this normalized template from an Asset Reconciliation Exclusion rule.

```
Apply AssetExclusion: Exclude DNS Name By IP on events which are detected
 by the Local system and NOT when any of
 Identity Host Name are contained in any of
 Asset Reconciliation DNS Whitelist - AlphaNumeric (Ignore Case),
 Asset Reconciliation DNS Blacklist - AlphaNumeric (Ignore Case)
 and when at least N1 events are seen with the same
 Identity Host Name and different Identity IP in N2
```

This table lists the variables in the rule template that can be tuned and the result of the change. Avoid changing other variables in the template.

**Table 56: Options for tuning the asset reconciliation rules**

Variable	Default value	Tuning result
N1	3	Tuning this variable to a lower value results in more data being added to the blacklist because fewer events with conflicting data are needed for the rule to fire. Tuning this variable to a higher value results in less data being added to the blacklist because more events with conflicting data are needed for the rule to fire.
N2	2 hours	Tuning this variable to a lower value reduces the window of time in which N1 events must be seen for the rule to fire. The time required to observe matching data is decreased, which results in less data being added to the blacklist. Tuning this variable to a higher value increases the time in which N1 events must be seen for the rule to fire. The time to observe matching data is increased, which results in more data being added to the blacklist. Increasing the time period might impact system memory resources as data is tracked over longer periods of time.

The Asset Reconciliation Exclusion rules are system-wide rules. Changes to the rules affect the way that the rule behaves throughout the entire system.

### *Applying different tuning for rules*

It might be necessary to apply different tuning for rules in different parts of the system. To apply different tuning for rules, you must duplicate the Asset Reconciliation Exclusion rules that you want to tune and add one or more tests to constrain the rules so that you test only certain parts of the system. For example, you might want to create rules that test only networks, log sources, or event types.

Always be cautious when you are adding new rules to the system because as some tasks and CRE rules might impact system performance. It might be beneficial to add the new rules to the top of each test stack to allow the system to bypass the remainder of the test logic whenever an asset update matches the criteria for the new rule.

- 1 Duplicate the rule.
  - a On the **Offenses** tab, click **Rules** and select the rule that you want to copy.
  - b Click **Actions > Duplicate**.  
It can be helpful if the name of the new rule is indicative of the reason for duplicating it.
- 2 Add a test to the rule.  
Determine a filter that you want to use to apply the rule only to a subset of system data. For example, you can add a test that matches only events from a specific log source.
- 3 Tune the variables of the rule to achieve the wanted behavior.
- 4 Update the original rule.
  - a Add the same test that you added to the duplicate rule to the original rule, but this time invert the rules **AND** and **AND NOT** operators.  
Inverting the operators prevents events from being triggered in both rules.



## Deleting invalid assets

After you fix the assets that contributed to the asset growth deviation, clean up your asset artifacts by using selective clean up or rebuilding the asset database.

**Selective clean up** This method is for asset growth deviations of limited scope. Selectively removing the affected assets is the least invasive way to clean up asset artifacts, but if many assets were affected, it can also be the most tedious.

**Rebuild the asset database** Rebuilding the asset database from scratch is the most efficient and precise method of deleting assets when asset growth deviations are pervasive.

This method passively regenerates assets in your database based on the new tuning that you configured to resolve the asset growth issues. With this approach, all scan results and residual asset data are lost, but the data can be reclaimed by rerunning a scan or re-importing scan results.

- 1 To selectively remove invalid artifacts in the asset database, perform these steps:
  - a On the **Log Activity** tab, run the **Deviating Asset Growth: Asset Report** event search.  
This search returns a report of assets that are affected by deviating asset growth and must be deleted.
  - b On the **Assets** tab, click **Actions > Delete Asset**  
There might be a delay before the asset no longer appears in Extreme Security.
- 2 To rebuild the asset database from scratch, perform these steps:
  - a Use SSH to log in to the Extreme Security Console as an administrator.
  - b Run the `/opt/qradar/support/cleanAssetModel.sh` script from the console command line and select **Option 1** when prompted.

Rebuilding the asset database restarts the asset reconciliation engine.

Purging a blacklist removes all blacklist entries, including those entries that were added manually. Blacklist entries that were manually added must be added again.

## Deleting blacklist entries

After you fixed the cause of the blacklist entries, you must clean up the remnant entries. You can remove the individual blacklist entries, however it is better to purge all blacklist entries and allow the blacklist values that are unrelated to the asset growth deviation to regenerate.

- 1 To purge a blacklist by using the Extreme Security Console:
  - a Click **Admin > System Configuration > Reference Set Management**.
  - b Select a reference set and then click **Delete**.
  - c Use the quick search text box to search for the reference sets that you want to delete, and then click **Delete Listed**.
- 2 To purge a blacklist by using the Extreme Security Console command-line interface:
  - a Change directory to `/opt/qradar/bin`.
  - b Run the following command.

```
./ReferenceDataUtil.sh purge "Reference Collection Name"
```

where *Reference Collection Name* is one of the following lists:

- Asset Reconciliation NetBIOS Blacklist
- Asset Reconciliation DNS Blacklist
- Asset Reconciliation IPv4 Blacklist
- Asset Reconciliation MAC Blacklist

Purging a blacklist removes all blacklist entries, including those entries that were added manually. Blacklist entries that were manually added must be added again.

## Modifying asset blacklists and whitelists

The asset blacklists and whitelists are reference sets. You can view and modify the asset blacklist and whitelist data using the **Reference Set Management** tool in the Extreme Security Console.

Alternatively, you can use the command line interface (CLI) or the RestFUL API endpoint to update the content of the asset blacklists and whitelists.

### Related Links

[Reference sets management](#)

## Updates to the asset blacklists and whitelists by using Extreme Security CLI

You can use the Extreme Networks Security Analytics command-line interface (CLI) to add or modify the entries that are on the asset blacklists or whitelists.

The commands to add new values to each list are described in the following table. The parameter values must exactly match the asset update values that are provided by the originating asset data source.

**Table 57: Command syntax to modify asset blacklist and whitelist data**

Name	Command syntax
Asset Reconciliation IPv4 Blacklist	<pre>ReferenceSetUtil.sh add "Asset Reconciliation IPv4 Blacklist" IP</pre> <p>For example, this command adds IP address 192.168.3.56 to the blacklist:</p> <pre>ReferenceSetUtil.sh add "Asset Reconciliation IPv4 Blacklist" 192.168.3.56</pre>
Asset Reconciliation DNS Blacklist	<pre>ReferenceSetUtil.sh add "Asset Reconciliation DNS Blacklist" DNS</pre> <p>For example, this command adds domain name 'misbehaving.asset.company.com' to the blacklist:</p> <pre>ReferenceSetUtil.sh add "Asset Reconciliation DNS Blacklist" "misbehaving.asset.company.com"</pre>
Asset Reconciliation NetBIOS Blacklist	<pre>ReferenceSetUtil.sh add "Asset Reconciliation NetBIOS Blacklist" NETBIOS</pre> <p>For example, this command removes NetBIOS host name 'deviantGrowthAsset-156384' from the blacklist:</p> <pre>ReferenceSetUtil.sh delete "Asset Reconciliation NetBIOS Blacklist" "deviantGrowthAsset-156384"</pre>

**Table 57: Command syntax to modify asset blacklist and whitelist data (continued)**

Name	Command syntax
Asset Reconciliation MAC Blacklist	<pre>ReferenceSetUtil.sh add "Asset Reconciliation MAC Blacklist" MACADDR</pre> <p>For example, this command adds MAC address '00:a0:6b:54:9f:0e' to the blacklist:</p> <pre>ReferenceSetUtil.sh add "Asset Reconciliation MAC Blacklist" "00:a0:6b:54:9f:0e"</pre>
Asset Reconciliation IPv4 Whitelist	<pre>ReferenceSetUtil.sh add "Asset Reconciliation IPv4 Whitelist" IP</pre> <p>For example, this command deletes IP address 10.1.95.142 from the whitelist:</p> <pre>ReferenceSetUtil.sh delete "Asset Reconciliation IPv4 Whitelist" 10.1.95.142</pre>
Asset Reconciliation DNS Whitelist	<pre>ReferenceSetUtil.sh add "Asset Reconciliation DNS Whitelist" DNS</pre> <p>For example, this command adds domain name 'loadbalancer.company.com' to the whitelist:</p> <pre>ReferenceSetUtil.sh add "Asset Reconciliation DNS Whitelist" "loadbalancer.company.com"</pre>
Asset Reconciliation NetBIOS Whitelist	<pre>ReferenceSetUtil.sh add "Asset Reconciliation NetBIOS Whitelist" NETBIOS</pre> <p>For example, this command adds NetBIOS name 'assetName-156384' to the whitelist:</p> <pre>ReferenceSetUtil.sh add "Asset Reconciliation NetBIOS Whitelist" "assetName-156384"</pre>
Asset Reconciliation MAC Whitelist	<pre>ReferenceSetUtil.sh add "Asset Reconciliation MAC Blacklist" MACADDR</pre> <p>For example, this command adds MAC address '00:a0:6b:54:9f:0e' to the blacklist:</p> <pre>ReferenceSetUtil.sh add "Asset Reconciliation MAC Blacklist" "00:a0:6b:54:9f:0e"</pre>

## Related Links

[Updating the blacklists and whitelists using the RESTful API](#) on page 155

## Updating the blacklists and whitelists using the RESTful API

You can use the Extreme Networks Security Analytics RESTful API to customize the content of the asset blacklists and whitelists.

You must specify the exact name of the reference set that you want to view or update.

- Asset Reconciliation IPv4 Blacklist
- Asset Reconciliation DNS Blacklist
- Asset Reconciliation NetBIOS Blacklist
- Asset Reconciliation MAC Blacklist
- Asset Reconciliation IPv4 Whitelist
- Asset Reconciliation DNS Whitelist
- Asset Reconciliation NetBIOS Whitelist
- Asset Reconciliation MAC Whitelist

- 1 Type the following URL in your web browser to access the RESTful API interface:

`https://ConsoleIPAddress/api_doc`

- 2 In the navigation pane on the left, find `4.0>/reference_data >/sets > /{name}`.
- 3 To view the contents of an asset blacklist or whitelist, follow these steps:
  - a Click the **GET** tab and scroll down to the **Parameters** section.
  - b In the **Value** field for the **Name** parameter, type the name of the asset blacklist or whitelist that you want to view.
  - c Click **Try It Out** and view the results at the bottom of the screen.
- 4 To add a value to an asset blacklist or whitelist, follow these steps:
  - a Click the **POST** tab and scroll down to the **Parameters** section.
  - b Type in the values for the following parameters:

**Table 58: Parameters that are required to add new asset data**

Parameter name	Parameter description
name	Represents the name of the reference collection that you want to update.
value	Represents the data item that you want to add to the asset blacklist or whitelist. Must exactly match the asset update values that are provided by the originating asset data source.

- c Click **Try It Out** to add the new value to the asset whitelist or asset blacklist.

For more information about using the RESTful API to change the reference sets, see the *Extreme Networks Security API Reference Guide*.

#### Related Links

[Updates to the asset blacklists and whitelists by using Extreme Security CLI](#) on page 154

You can use the Extreme Networks Security Analytics command-line interface (CLI) to add or modify the entries that are on the asset blacklists or whitelists.

# 13 Configuring QRadar systems to forward data to other systems

---

Adding forwarding destinations  
Configuring forwarding profiles  
Configuring routing rules for bulk forwarding  
Configuring selective forwarding  
Viewing forwarding destinations  
Viewing and managing forwarding destinations  
Viewing and managing routing rules

You can configure Extreme Networks Security Analytics systems to forward data to one or more vendor systems, such as ticketing or alerting systems. You can also forward normalized data to other Extreme Security systems. The target system that receives the data from Extreme Security is known as a *forwarding destination*.

With exception of domain tagging, Extreme Security systems ensure that all forwarded data is unaltered. Domain information is removed from forwarded data. Events that contain domain information are automatically assigned to the default domain on the receiving system.

To avoid compatibility problems when sending event data, ensure that the deployment receiving the data is the same version or higher than the deployment that is sending the data.

- 1 Configure one or more forwarding destinations.
- 2 To determine what data you want to forward, configure routing rules, custom rules, or both.
- 3 Configure the routing options to apply to the data.

For example, you can configure all data from a specific event collector to forward to a specific ticketing system. You can also bypass correlation by removing the data that matches a routing rule.

## Adding forwarding destinations

---

Before you can configure bulk or selective data forwarding, you must add forwarding destinations.

- 1 Click the **Admin** tab.
- 2 In the navigation pane, click **System Configuration**.
- 3 Click the **Forwarding Destinations** icon.
- 4 On the toolbar, click **Add**.
- 5 In the **Forwarding Destinations** window, enter values for the parameters.

The following table describes some of the **Forwarding Destinations** parameters.

**Table 59: Forwarding Destinations parameters**

Parameter	Description
Event Format	<ul style="list-style-type: none"> <li><b>Payload</b> is the data in the format that the log source sent.</li> <li><b>Normalized</b> is raw data that is parsed and prepared as readable information for the user interface.</li> </ul>
Destination Address	The IP address or host name of the vendor system that you want to forward data to.
Protocol	<ul style="list-style-type: none"> <li><b>TCP</b> Use the <b>TCP</b> protocol to send normalized data by using the TCP protocol, you must create an off-site source at the destination address on port 32004.</li> <li><b>UDP</b></li> </ul>
Prefix a syslog header if it is missing or invalid	<p>If a valid syslog header is not detected on the original syslog message, select this check box. The prefixed syslog header includes the Extreme Security appliance host IP address in the <b>Hostname</b> field of the syslog header. If this check box is not selected, the data is sent unmodified.</p> <p>When Extreme Security forwards syslog messages, the outbound message is verified to ensure that it has a valid syslog header.</p>

6 Click **Save**.

## Configuring forwarding profiles

If you want to specify which properties to forward to the forwarding destination, configure a forwarding profile.

You must re-create JSON forwarding profiles that you created in Extreme Networks Security Analytics V7.2.3 or earlier.

You can use forwarding profiles only when the event data is sent in JSON format.

You can select specific event properties, including custom properties, to forward to an external destination. You can enhance the readability of the event data by specifying an alias name and default value for the attribute. Alias names and default values are specific to the profile they are defined in. If the attributes are used in other profiles, the alias names and default values must be redefined.

You can use a single profile that has multiple forwarding destinations. When you edit a profile, ensure that the changes are appropriate for all forwarding destinations that the profile is associated with.

When you delete a profile, all forwarding destinations that used the profile automatically revert to using the default profile.

- 1 Click the **Admin** tab, and in the navigation pane, click **System Configuration**.
- 2 Click the **Forwarding Destinations** icon.
- 3 On the toolbar, click **Profile Manager**.
- 4 To create a new profile, click **New**.
- 5 Type a name for the profile and select the check box beside the attributes that you want to include in the event data set.
- 6 To change an existing profile, select the profile and click **Edit** or **Delete**.

- 7 Click **Save**.

## Configuring routing rules for bulk forwarding


After you added one or more forwarding destinations, you can create filter-based routing rules to forward large quantities of data.

You can configure routing rules to forward data in either online or offline mode:

- In **Online** mode, your data remains current because forwarding is performed in real time. If the forwarding destination becomes unreachable, data can potentially be lost.
- In **Offline** mode, all data is stored in the database and then sent to the forwarding destination. This assures that no data is lost, however, there might be delays in data forwarding.

The following table describes some of the **Routing Rules** parameters

**Table 60: Routing Rules window parameters**

Parameter	Description
Forwarding Event Collector	This option is displayed when you select the <b>Online</b> option. Specifies the Event Collector that you want this routing rule process data from.
Forwarding Event Processor	This option is displayed when you select the <b>Offline</b> option. Specifies the Event Processor that you want this routing rule process data from.
	 <b>Note</b> This option is not available if <b>Drop</b> is selected from the <b>Routing Options</b> pane.
Routing Options	<ul style="list-style-type: none"> <li>• The <b>Forward</b> option specifies that data is forwarded to the specified forwarding destination. Data is also stored in the database and processed by the Custom Rules Engine (CRE).</li> <li>• The <b>Drop</b> option specifies that data is not stored in the database and is not processed by the CRE. The data is not forwarded to a forwarding destination, but it is processed by the CRE. This option is not available if you select the <b>Offline</b> option.</li> <li>• The <b>Bypass Correlation</b> option specifies that data is not processed by the CRE, but it is stored in the database. This option is not available if you select the <b>Offline</b> option.</li> </ul> <p>You can combine two options:</p> <ul style="list-style-type: none"> <li>• <b>Forward and Drop</b>  Data is forwarded to the specified forwarding destination. Data is not stored in the database and is processed by the CRE.</li> <li>• <b>Forward and Bypass Correlation</b>  Data is forwarded to the specified forwarding destination. Data is also stored in the database, but it is not processed by the CRE. The CRE at the forwarded destination processes the data.</li> </ul> <p>If data matches multiple rules, the safest routing option is applied. For example, if data that matches a rule that is configured to drop and a rule to bypass CRE processing, the data is not dropped. Instead, the data bypasses the CRE and is stored in the database. All events are counted against the EPS license.</p>

- 1 Click the **Admin** tab.
- 2 In the navigation pane, click **System Configuration**.

- 3 Click the **Routing Rules** icon.
- 4 On the toolbar, click **Add**.
- 5 In the **Routing Rules** window, enter values for the parameters.
  - a Type a name and description for your routing rule.
  - b From the **Mode** field, select one of the following options: **Online** or **Offline**.
  - c From the **Forwarding Event Collector** or **Forwarding Event Processor** list, select the event collector from which you want to forward data.
  - d To forward all incoming data, select the **Match All Incoming Events** check box.

**Note**

If you select this check box, you cannot add a filter.

- e To add a filter, in the **Event Filters** section, select a filter from the first list and an operand from the second list.
- f In the text box, type the value that you want to filter for, and then click **Add Filter**.
- g Repeat the previous two steps for each filter that you want to add.
- h To forward log data that matches the current filters, select the **Forward** check box, and then select the check box for each preferred forwarding destination.

**Note**

If you select the **Forward** check box, you can also select either the **Drop** or **Bypass Correlation** check boxes, but not both of them.

If you want to edit, add, or delete a forwarding destination, click the **Manage Destinations** link.

- 6 Click **Save**.

## Configuring selective forwarding

Use the **Custom Rule** wizard to configure highly selective event data forwarding. Configure rules that forward event data to one or more forwarding destinations as a rule response.

The criteria that determines the event data that is sent to a forwarding destination is based on the tests and building blocks that are included in the rule. When the rule is configured and enabled, all event data that matches the rule tests are automatically sent to the specified forwarding destinations. For more information about how to edit or add a rule, see the *User Guide* for your product.

- 1 Click the tab.
- 2 From the Rules menu, select **Rules**.
- 3 Edit or add a rule. On the **Rule Response** page in the **Rule** wizard, ensure that you select the **Send to Forwarding Destinations** option.

## Viewing forwarding destinations

The **Forwarding Destinations** window provides valuable information about your forwarding destinations. Statistics for the data sent to each forwarding destination is displayed.

For example, you can see the following information:



- The total number events that were seen for this forwarding destination.
- The number of events that were sent to this forwarding destination.
- The number of events that were dropped before the forwarding destination was reached.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration**.
- 3 Click the **Forwarding Destinations** icon.
- 4 View the statistics for your forwarding destinations.

## Viewing and managing forwarding destinations

Use the **Forwarding Destination** window to view, edit, and delete forwarding destinations.

- 1 Click the **Admin** tab.
- 2 In the navigation pane, click **System Configuration**.
- 3 Click the **Forwarding Destinations** icon.

Statistics for the data sent to each forwarding destination is displayed. For example, you can see the following information:

- The total number events that were seen for this forwarding destination.
  - The number of events that were sent to this forwarding destination.
  - The number of events that were dropped before the forwarding destination was reached.
- 4 On the toolbar, click an action, as described in the following table.

**Table 61: Description of the Forwarding Destination toolbar actions**

Action	Description
	Changes the configured name, format, IP address, port, or protocol

## Viewing and managing routing rules

The **Event Routing Rules** window provides valuable information about your routing rules. You can view or manage configured filters and actions when data matches each rule.

Use the **Event Routing Rules** window to edit, enable, disable, or delete a rule. You can edit a routing rule to change the configured name, Event Collector, filters, or routing options.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration**.
- 3 Click the **Routing Rules** icon.
- 4 Select the routing rule you want to manage.
- 5 To edit the routing rule, on the toolbar, click **Edit** and update the parameters.
- 6 To remove the routing rule, on the toolbar, click **Delete**.
- 7 To enable or disable the routing rule, on the toolbar, click **Enable/Disable**.

If you enable a routing rule that is configured to drop events, a confirmation message is displayed.

# 14 Event store and forward

## Store and forward overview

### Viewing the Store and Forward schedule list

### Creating a new Store and Forward schedule

### Editing a Store and Forward schedule

### Deleting a Store and Forward schedule

Use the Store and Forward feature to manage schedules for forwarding events from your dedicated Event Collector appliances to Event Processor components in your deployment.

The Store and Forward feature is supported on the Event Collector 1501 and Event Collector 1590. For more information about these appliances, see the *Extreme Networks Security Hardware Guide*.

A dedicated Event Collector does not process events and it does not include an on-board Event Processor. By default, a dedicated Event Collector continuously forwards events to an Event Processor that you must connect by using the **Deployment Editor**. Use the Store and Forward feature to schedule a time range for when you want the Event Collector to forward events. During the time when events are not forwarding, the events are stored locally on the appliance. The events are not accessible in the Extreme Security Console user interface.

Use the scheduling feature to store events during your business hours. Forward the events to an Event Processor when the transmission does not negatively affect your network bandwidth. For example, you can configure an Event Collector to forward events to an Event Processor during non-business hours.

## Store and forward overview

The Store and Forward feature is supported on the Event Collector 1501 and Event Collector 1590 appliances. For more information on these appliances, see the *QRadar Hardware Guide*.

A dedicated Event Collector does not process events and it does not include an on-board Event Processor. By default, a dedicated Event Collector continuously forwards events to an Event Processor that you must connect using the Deployment Editor. The Store and Forward feature allows you to schedule a time range for when you want the Event Collector to forward events. During the period of time when events are not forwarding, the events are stored locally on the appliance and are not accessible using the Console user interface.

This scheduling feature allows you to store events during your business hours and then forward the events to an Event Processor during periods of time when the transmission does not negatively affect your network bandwidth. For example, you can configure an Event Collector to only forward events to an Event Processor during non-business hours, such as midnight until 6 AM.

## Viewing the Store and Forward schedule list

Use the **Store and Forward** window to see a list of schedules. The schedules include statistics that help you evaluate the status, performance, and progress of your schedules.

You must create a schedule. By default, the first time that you access the **Store and Forward** window, no schedules are listed.


You can use options on the toolbar and the **Display** list box to change your view of the schedule list. Change your view of the list to focus on the statistics from various points of view. For example, if you want to view the statistics for a particular Event Collector, you can select **Event Collectors** from the **Display** list. The list then groups by the **Event Collector** column and makes it easier for you to locate the Event Collector that you want to investigate.

By default, the Store and Forward list is configured to display the list that is organized by the schedule (**Display > Schedules**).






- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration**.
- 3 Click the **Store and Forward** icon.
- 4 In the **Store and Forward** window, view the parameters for each schedule.

The following table describes some of the parameters for the schedule.


**Table 62: Store and Forward window parameters**

Parameter	Description
Display	<p>The <b>Schedules</b> option shows a hierarchy of the parent-child relationship between the schedules, Event Processors and the associated Extreme Security Event Collectors.</p> <p>The <b>Event Collectors</b> option shows the lowest level in the hierarchy, which is a list of Extreme Security Event Collectors.</p> <p><b>Event Processors</b> option shows a hierarchy of the parent-child relationship between the Event Processors and the associated Extreme Security Event Collectors.</p>
Name	<p>For the <b>Schedules</b> option, the <b>Name</b> column is displayed the following format.</p> <ul style="list-style-type: none"> <li>• <b>First Level</b> represents the name of the schedule.</li> <li>• <b>Second Level</b> represents the name of the Event Processor.</li> <li>• <b>Third Level</b> represents the name of the Event Collector.</li> </ul> <p>For the <b>Event Processors</b> option, the column is displayed in the following format</p> <ul style="list-style-type: none"> <li>• <b>First Level</b> represents the name of the Event Processor.</li> <li>• <b>Second Level</b> represents the name of the Event Collector.</li> </ul> <div style="border-top: 1px solid black; padding-top: 10px;"> <p> <b>Tip</b> You can use the plus symbol (+) and minus symbol (-) beside the name or options on the toolbar to expand and collapse the hierarchy tree. You can also expand and collapse the hierarchy tree by using options on the toolbar.</p> </div>

**Table 62: Store and Forward window parameters (continued)**

Parameter	Description
Schedule Name	<p>Displays the name of the schedule for the <b>Event Collectors</b> or <b>Event Processors</b> options. If an Event Processor is associated with more than one schedule, the <b>Schedule Name</b> shows <b>Multiplen</b>, where <i>n</i> is the number of schedules.</p> <hr/> <p> <b>Tip</b> Click the plus symbol (+) to view the associated schedules.</p> <hr/>
Last Status	<p>Displays the status of the Store and Forward process:</p> <ul style="list-style-type: none"> <li>• <b>Forwarding</b> indicates that event forwarding is in progress.</li> <li>• <b>Forward Complete</b> indicates that event forwarding is successfully completed and events are stored locally on the Event Collector. The stored events are forwarded when the schedule indicates that forwarding can start again.</li> <li>• <b>Warn</b> indicates that the percentage of events that are remaining in storage exceeds the percentage of time that is remaining in the Store and Forward schedule.</li> <li>• <b>Error</b> indicates that event forwarding was stopped before all stored events were forwarded.</li> <li>• <b>Inactive</b> indicates that no Extreme Security Event Collectors are assigned to the schedule, or the assigned Extreme Security Event Collectors are not receiving any events.</li> </ul> <hr/> <p> <b>Tip</b> Move your mouse pointer over the <b>Last Status</b> column to view a summary of the status.</p> <hr/>
Forwarded Events	<p>Displays the number of events (in K, M, or G) forwarded in the current session.</p> <hr/> <p> <b>Tip</b> Move your mouse pointer over the value in the <b>Forwarded Events</b> column to view the number of events.</p> <hr/>
Remaining Events	<p>Displays the number of events (in K, M, or G) remaining to be forwarded in the current session.</p> <hr/> <p> <b>Tip</b> Move your mouse pointer over the value in the <b>Remaining Events</b> column to view the number of events.</p> <hr/>
Average Event Rate	<p>Displays the average rate at which events are forwarding from the Event Collector to the Event Processor.</p> <hr/> <p> <b>Tip</b> Move your mouse pointer over the value in the <b>Average Event Rate</b> column to view the average events per second (EPS).</p> <hr/>

**Table 62: Store and Forward window parameters (continued)**

Parameter	Description
Current Event Rate	Displays the rate at which events are forwarding from the Event Collector to the Event Processor
	 <b>Tip</b> Move your mouse pointer over the value in the <b>Current Event Rate</b> column to view the current events per second (EPS)
Transfer Rate Limit	The transfer rate limit is configurable. The transfer rate limit can be configured to display in kilobit per second (kbps), megabits per second (Mbps), or gigabits per second (Gbps).

## Creating a new Store and Forward schedule

Use the Store and Forward Schedule wizard to create a schedule that controls when your Event Collector starts and stops forwarding data to an Event Processor.

You can create and manage multiple schedules to control event forwarding from multiple Extreme Security Event Collectors in a geographically distributed deployment.

Ensure that your dedicated Event Collector is added to your deployment and connected to an Event Processor. The connection between an Event Collector and an Event Processor is configured in the **Deployment Editor**.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration**.
- 3 Click the **Store and Forward** icon.
- 4 Click **Actions > Create**.
  - a Click **Next** to move to the **Select Collectors** page.
  - b On the **Select Collectors** page, configure the parameters.  
If the Event Collector that you want to configure is not listed, it might not be added to your deployment. If so, use the **Deployment Editor** to add the Event Collector and then proceed.
  - c On the **Schedule Options** page, configure the parameters.  
To configure the forward transfer rate, the minimum transfer rate is 0. The maximum transfer rate is 9,999,999. A value of 0 means that the transfer rate is unlimited.
  - d Finish the configuration.  
You can now view the schedule in the **Store and Forward** window. After you create a new schedule, it might take up to 10 minutes for statistics to start displaying in the **Store and Forward** window.

## Editing a Store and Forward schedule

You can edit a **Store and Forward** schedule to add or remove Extreme Security Event Collectors and change the schedule parameters. After you edit a **Store and Forward** schedule, the statistics that are displayed in the **Store and Forward** list are reset.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration**.
- 3 Click the **Store and Forward** icon.
- 4 Select the schedule that you want to edit.
- 5 Click **Actions > Edit**.  
You can also double-click a schedule for editing.
- 6 Click **Next** to move to the **Select Collectors** page.
- 7 On the **Select Collectors** page, edit the parameters.
- 8 Click **Next** to move to the **Schedule Options** page.
- 9 On the **Schedule Options** page, edit the scheduling parameters.
- 10 Click **Next** to move to the **Summary** page.
- 11 On the **Summary** page, confirm the options that you edited for this schedule.

After you edit a schedule, it might take up to 10 minutes for statistics to update in the **Store and Forward** window.

## Deleting a Store and Forward schedule

---

You can delete a **Store and Forward** schedule.

- 1 On the navigation menu, click **System Configuration**.
- 2 Click the **Store and Forward** icon.
- 3 Select the schedule that you want to delete.
- 4 Click **Actions > Delete**.

After the schedule is deleted, the associated Extreme Security Event Collectors resume continuous forwarding of events to their assigned Event Processor.

# 15 Content Management Tool overview

---

Exporting all custom content  
Exporting all custom content of a specific type  
Searching for content  
Exporting multiple custom content items  
Exporting a single custom content item  
Importing custom content  
Updating content  
Content Management Tool audit details

Using the Content Management Tool (CMT), you can export security and configuration content from Extreme Networks Security Analytics into an external, portable format.

You can import the exported content into the same system you exported from or into another Extreme Security system.

You can export and import the following content:

- Dashboards
- Reports
- Groups
- Saved Searches
- Reference Data collections, including Reference Sets
- Custom and Calculated Properties
- Custom Rules and Building Blocks
- Log Source
  - Log Source types
  - Log Source categories
  - Log Source extensions
  - Log Source Groups
- Rule/Building Block Groups
- Reporting Groups
- Search Groups
  - Event Search Groups

You cannot use CMT to import and export saved search criteria for Offense, Assets, and Vulnerability.

The following parameters always behave the same regardless of the value of the `--action` parameter that you use.

**Table 63: Parameters for CMT**

Parameter	Description
<code>-h [--help]</code> <i>ACTIONTYPE</i>	Displays help that is specific to the ACTIONTYPE option or general help message if no ACTIONTYPE option is specified.
<code>-q [--quiet]</code>	No output appears on screen when CMT runs.
<code>-v [--verbose]</code>	Use verbose level when you log in to view default-level CMT information.
<code>-d [--debug]</code>	Use debug level when you log in to see more detailed information, such as logs for customer support.

If no valid ACTIONTYPE option is available, the CMT displays general help. If the ACTIONTYPE is valid, the CMT displays the action-specific help.

When you import and export *custom content*, the CMT checks content dependencies, and then includes associated content in the import or export. For example, when the CMT detects that a custom report is associated with custom saved searches, the custom saved searches are also exported.

## Exporting all custom content

Export all custom content in a single action with the Content Management Tool (CMT).

- 1 Using SSH, log in to Extreme Networks Security Analytics as the root user.
- 2 Go to `/opt/qradar/bin` directory, and export the content:

```
cd /opt/qradar/bin
```

- To export all content that excludes data accumulation references, type the following command:

```
./contentManagement.pl -a export -c all
```

- To export all the content that includes accumulated data, type the following command:

```
./contentManagement.pl -o [directory_path] -a export -c all -g
```

If no output directory is specified when you use the `-o` option, the content is exported to the user's current directory. If the specified directory does not exist, it is created.

The exported content is compressed to a `.tar.gz` file and exported to the specified directory. The following example shows a `.tar.gz` file name: `report-ContentExport-20120419101803.tar.gz`. You can manually change the name of the exported file.

The following table describes the parameters used in commands for exporting all custom content.



**Table 64: Export parameters (all custom content)**

Parameter	Description
-a export	The action to be executed.
-o PATH	The directory where the content is written. If the directory is not specified, the user's current directory is used.
-g	Include accumulated data in the export.

## Exporting all custom content of a specific type

Export all custom content of a specific type in one action, rather than exporting content items individually.

- 1 Using SSH, log in to Extreme Networks Security Analytics as the root user.
- 2 Go to `/opt/gradar/bin` and export content of a specific type:
  - To export all custom content of a specific type, type the following command:

```
./contentManagement.pl --action export --content-type Content_Type --id all
```

- To export all custom content that includes accumulated data, type the following command:

```
./contentManagement.pl --action export --content-type Content_Type --id all --global-view
```

The following table describes the parameters in commands to export custom content of a specific type.

**Table 65: Export parameters (custom content of a specific type)**

Parameter	Description
-c CONTENT_TYPE	The type of content that you want to import or export. You can type the content type as a text string or type the corresponding numeric identifier. See <a href="#">Content types</a> .
-o PATH	The directory where the content is written. If not specified the user's current directory is used.
-i	The identifier of a specific instance of custom content, such as a single report or a single reference set. Specify <b>All</b> to export all content of the provided content-type.
-g	Include accumulated data in the export.

**Table 66: Content types**

Custom Content Type	Text String	Numeric Identifier
All custom content	<code>all</code>	n/a
Custom list of content	<code>package</code>	n/a
Dashboard	<code>dashboard</code>	4
Reports	<code>report</code>	10
Saved Searches	<code>search</code>	1
FGroup <sup>1</sup>	<code>fgroup</code>	12
FGroup Type	<code>fgrouptype</code>	13
Custom Rules	<code>customrule</code>	3
Custom Properties	<code>customproperty</code>	6
Log Source	<code>sensordevice</code>	17
Log Source Type	<code>sensordevicetype</code>	24
Log Source Category	<code>sensordevicecategory</code>	18
Log Source Extensions	<code>deviceextension</code>	16
Reference data collections	<code>referencedata</code>	28
<sup>1</sup> An FGroup represents a group of content, such as a log source group, reporting group, or search group. These groups can be log activity event search groups, report groups, vulnerability management search groups, or log source groups.		

The export bundle contains more data items than the user selected, because each item exports with all dependencies.

The exported content is compressed to a .tar.gz file and exported to the specified directory. You can also manually change the name of the exported file.

## Searching for content

Use the `search` command to query your custom content for unique string ID values. You need this information when you export a specific instance of custom content such as a single report or a single reference set, or if a package contains different content-type IDs.

- 1 Using SSH, log in to Extreme Networks Security Analytics as the root user.
- 2 Go to `/opt/qradar/bin` and search for custom content:

```
./contentManagement.pl -a search -c content-type -r regex
```

### Example

```
/opt/qradar/bin/contentManagement.pl --action search
--content-type customrule --regex "PCI.*"
```

```
/opt/qradar/bin/contentManagement.pl --action search
--content-type dashboard --regex "Overview.*"
```

The following table describes parameters used in Content Management Tool (CMT) search commands.

**Table 67: Search parameters**

Parameter	Description
<code>-c</code> or <code>--content-type content-type</code>	The text string or numeric identifier of the type of content to export. The value can be anything from the content type table.
<code>-r</code> or <code>--regex regex</code>	The regular expression (regex) is used to search a content-type. All matching content is displayed.

**Table 68: CMT Content types**

Custom content type	Text string	Numeric identifier
Dashboard	dashboard	4
Reports	report	10
Saved Searches	search	1
FGroup	fgroup	12
FGroup Type	fgrouptype	13
Custom Rules	customrule	3
Custom Properties	customproperty	6
Log Source	sensordevice	17
Log Source Type	sensordevicetype	24
Log Source Category	sensordevicecategory	18
Log Source Extensions	deviceextension	16
Reference data collections	referencedata	28

## Exporting multiple custom content items

Export multiple custom content items in the same action, such as custom rules, with the Content Management Tool (CMT).

- 1 Using SSH, log in to Extreme Networks Security Analytics as the root user.

- 2 Create a package file, including all required custom content items. Each custom content item is made up of an export content type, followed by a comma-separated list of IDs.

#### Example

A user wants to export two dashboards, which have ID 5 and ID 7, all custom rules, and a group. The file that is stored in the `/root/myPackage` directory contains the following entries:

```
dashbord, 5,7

customrule,all

fgroup, 77
```

- 3 Go to `/opt/qradar/bin`, and export and save all items:
  - If you want to export all items in the `/root/myPackage` file and save the exported content in the current directory, type the following command:

```
./contentManagement.pl -a export -c package -f /root/myPackage
```

- If you want to export all items in the `/root/myPackage` file, which includes accumulated data, and save the output in the `/store/cmt/exports` directory, type the following command:

```
./contentManagement.pl --action export --content-type package --file
/root/myPackage --output-directory /store/cmt/exports --global-view
```

The exported content is compressed to a `.tar.gz` file and exported on to the specified directory, or the user's current directory. You can manually change the name of the exported file.

After you use a package file, a package template is written to `/store/cmt/packages`. A package file is reusable, and can be stored anywhere.

**Table 69: Export parameters (multiple custom content items)**

Parameter	Description
<code>-a [--action] export</code>	The action to be executed.
<code>-c [--content-type] package</code>	The content type to be exported. The "package" option is the required content-type.
<code>-f [--file] FILE</code>	The file path and file name, such as <code>/root/myPackage</code> of the package file, which contains custom content items. Enter one file for each line. The export type is followed by a list of one or more IDs.
<code>-o [--output-directory] PATH</code>	The directory where the content is written. If the directory is not specified, the user's current directory is used.

## Exporting a single custom content item

Export a single custom content item, such as a custom rule or a custom search criteria.

- 1 Using SSH, log in to Extreme Networks Security Analytics as the root user.

2 Go to the `cd /opt/gradar/bin` and export a single custom content item:

- To export a single custom content item that excludes accumulated data, type the following command:

```
./contentManagement.pl -a export -o <directory_path> -c
<content_type> -i string_ID_value
```

- To export a single custom content item that includes accumulated data, type the following command:

```
./contentManagement.pl -a export -o <directory_path> -c
<content_type> -i string_ID_value -g
```

**Table 70: Export parameters (single content item)**

Parameters	Description
<code>-o directory_path</code>	The directory to which you want to export content. If an output directory is not specified, the content is exported to the user's current directory.
<code>-c content_type</code>	The type of content that you want to export. You can type the content type as a text string or type the corresponding numeric identifier. See <a href="#">Content Types</a> .
<code>-a</code>	Specifies whether you want to export the specified custom content.
<code>-i string_ID_value</code>	The identifier for the specific instance of custom content, such as a single report or a single reference set. You can locate the <code>string_ID_value</code> by querying the PostgreSQL database with the CMT search option.

The exported content is compressed to a `.tar.gz` file and exported to the specified directory. You can manually change the name of the exported file.

## Importing custom content

You can import custom content into the same Extreme Networks Security Analytics system that you exported from or you can import into another Extreme Security system.

If you want to import the content into another Extreme Security system, you must transfer the output file to the other system before you proceed with this procedure.

The Content Management Tool (CMT) converts imported files to the local Extreme Security version if required. The import action imports content that is not already on the system. When you import content bundles that have log sources, confirm that DSM and protocol RPMs are installed and current on the target system.



### Note

Do not start multiple imports on the same system at the same time.

1 Using SSH, log in to Extreme Security as the root user.

- 2 Go to the directory where you exported the content file.

```
cd directory_name
```

- 3 To list the files in the directory, type the following command:

```
ls-al
```

The output of this command resembles the following example:

```
drwxr-xr-x 2 root root 24576 Apr 18 16:39
fgroup-ContentExport-20120418163707

-rw-r-r- 1 root root 324596 Apr 18 16:39
fgroup-ContentExport-20120418163707.tar.gz

drwxr-xr-x 2 root root 4096 Apr 18 16:56
report-ContentExport-20120418165529

-rw-r-r- 1 root root 42438 Apr 18 16:56
report-ContentExport-20120418165529.tar.gz

drwxr-xr-x 2 root root 4096 Apr 19 10:18
report-ContentExport-20120419101803

-rw-r-r- 1 root root 3295 Apr 19 10:18
report-ContentExport-20120419101803.tar.gz
```

In this example, `report-ContentExport-20120419101803.tar.gz` is an export file name.

If you uncompress the `.tar.gz` file manually while the file is in the default or custom export directory, you must move the extracted files and directories to another location before you import the `tar.gz` file.

- 4 Type the following command:

```
/opt/qradar/bin/contentManagement.pl -a import -f export_file_path
```

### Example

```
/opt/qradar/bin/contentManagement.pl --action import

--file fgroup-ContentExport-20120418163707.tar.gz
```

**Table 71: Import parameters**

Parameter	Description
-a	The action to be executed.
-f <i>export_file_path</i>	The file that contains the exported content data. This file is either a compressed <code>tar.gz</code> , or a file that contains the XML representation of the exported content. If the files are described in the XML representation file, report or logo, or both, files must also appear in a subdirectory. Use the path included in the XML representation. The file option is either an absolute path or a relative path to the users current directory.

CMT uses the following parameters to confirm that it imports the correct record.

**Table 72: Import parameters**

Custom content type	Uniqueness key
Dashboard	Name and owner
Reports	N/A, reports are always unique
Saved Search - customviewparams	ID
Group (FGroup)	Name and parent_id
Group type (FGroup type)	Name
Custom rule	UUID
Custom properties	propertyname
Log Source	devicename and eccomponentid
Log Source Type	devicetypename
Log Source Category	ID
Log Source extensions	Name
Reference Data	ID

- If the user list on the source system is different from the user list on the target system, CMT adds all data to the target system.
- CMT displays the following error when you import and update Reference Data: **Foreign key constraint violation**. This error is caused by data actively collected during the export of reference data. To avoid this issue, run the export process when no reference data is being collected.

## Updating content

Use the update action to update existing content, and add new content to the system.

When you import content bundles that have log sources, confirm that DSM and Protocol RPMs are installed and current on the target system.

- 1 Using SSH, log in to Extreme Networks Security Analytics as the root user.
- 2 To update the exported file, go to the directory where you exported the content file and type the following command:

```
/opt/qradar/bin/contentManagement.pl -a update -f export_file_path
```

### Example

```
/opt/qradar/bin/contentManagement.pl
```

```
-a update --file fgroup-ContentExport-20120418163707.tar.gz
```

**Table 73: Update parameters**

Parameter	Description
<b>-a or --action update</b>	Changes the information on the system.
<b>-f or --file</b>	The compressed <code>tar.gz</code> file that contains the exported content data. The file option can be an absolute or relative path to the current directory of the user.

## Content Management Tool audit details

Use the audit events generated by the content management tool (CMT) to confirm correct content exports and imports.


### Audit details for all actions

The following table lists audit events that are created for export, import, search, and update actions. The audit output contains information for the following audit events:

- Shell user
- Remote IP
- List of arguments that are passed as the event payload

The normalized event fields for the audit are `Source IP = Remote IP`, `User = Shell User`.

**Table 74: Audit details**

Action/Audit event name	Event name	Event description
ExportInitiated	Content Export Initiated	User initiated content export
ExportComplete	Content Export Complete	Content export is complete
<div>  <p><b>Note</b> Also includes list of arguments that are exported in the audit output</p> </div>		
ImportInitiated	Content Import Initiated	User initiated content import



**Table 74: Audit details (continued)**

Action/Audit event name	Event name	Event description
ImportComplete	Content Import Complete	Content import is complete
UpdateInitiated	Content Update Initiated	User initiated content update
UpdateComplete	Content Update Complete	Content update is complete
SearchInitiated	Content Search Initiated	User initiated content search

## Audit events for import and update actions

The following audit events are generated when you import or update content.

**Table 75: Import and update audit events**

Action / Audit event name	Event name	Output details, string representation
ArielProperty	ArielPropertyAdded	what was added
ArielProperty	ArielPropertyModified	what was modified
QidMap	QidMapEntryAdded	what was added
QidMap	QidMapEntryModified	what was modified
DeviceExtension	DeviceExtensionAdded	what was added
DeviceExtension	DeviceExtensionModified	what was modified
DeviceExtension	DeviceExtension AssociationModified	what was modified
DeviceExtension	DeviceExtension AssociationModified	what was modified
Sensordevice	SensorDeviceAdded	what was added
Sensordevice	SensorDeviceModified	what was modified
ReferenceData	ReferenceDataCreated	what was added
ReferenceData	ReferenceDataUpdated	what was updated
Fgroup	FgroupAdded	what was added
Fgroup	FgroupModified	what was modified
Fgroup	FgroupItemsAdded	what was added
CRE	RuleAdded	what was added
CRE	RuleModified	what was modified
Retention	RetentionSettingsUpdated	what was modified
Dashboard	DashboardAdded	what was added
Reports	ReportAdded	what was added
Reports	ReportModified	what was modified

# 16 SNMP trap configuration

## Customizing the SNMP trap information sent to another system

### Customizing the SNMP trap output

### Adding a custom SNMP trap to Extreme Security

### Sending SNMP traps to a specific host

In , you can configure a rule to generate a rule response that sends an SNMP trap when configured conditions are met. acts as an agent to send the SNMP traps to another system.

A Simple Network Management Protocol (SNMP) trap is an event or offense notification that sends to a configured SNMP host for additional processing.

Customize the SNMP configuration parameters in the custom rules wizard and modify the SNMP traps that the custom rule engine sends to other software for management. provides two default traps. However, you can add custom traps or modify the existing traps to use new parameters.

For more information on SNMP, go to the [The Internet Engineering Task Force](http://www.ietf.org/) (<http://www.ietf.org/>) website and type RFC 1157 in the search field.

## Customizing the SNMP trap information sent to another system

In Extreme Networks Security Analytics, you can edit the SNMP trap parameters to customize the information that is sent to another SNMP managing system when a rule condition is met.



### Note

The SNMP trap parameters are displayed in the custom rules wizard only if SNMP is enabled in the Extreme Security system settings.

- 1 Use SSH to log in to Extreme Security as the root user.
- 2 Go to the `/opt/qradar/conf` directory and make backup copies of the following files:
  - `eventCRE.snmp.xml`
  - `offenseCRE.snmp.xml`
- 3 Open the configuration file for editing.
  - To edit the SNMP parameters for event rules, open the `eventCRE.snmp.xml` file.
  - To edit the SNMP parameters for offense rules, open the `offenseCRE.snmp.xml` file.
- 4 Inside the `<snmp>` element and before the `<creSNMPTrap>` element, insert the following section, updating the labels as needed:

```
<creSNMPResponse name="snmp_response_1">
 <custom name="MyColor">
 <string label="What is your favorite color?"/>
 </custom>
 <custom name="MyCategory">
```

```

 <list label="Select a category">
 <option label="Label1" value="Category1"/>
 <option label="Label2" value="Category2"/>
 </list>
 </custom>
</creSNMPResponse>

```

- 5 Save and close the file.
- 6 Copy the file from the `/opt/qradar/conf` directory to the `/store/configservices/staging/globalconfig` directory.
- 7 Log in to the Extreme Security interface.
- 8 On the **Admin** tab, select **Advanced** > **Deploy Full Configuration**.

When you deploy the full configuration, Extreme Security restarts all services. Data collection for events stops until the deployment completes.

Customize the SNMP trap output..

## Customizing the SNMP trap output

Extreme Networks Security Analytics uses SNMP to send traps that provide information when rule conditions are met.

By default, Extreme Security uses the Extreme Security management information base (MIB) to manage the devices in the communications network. However, you can customize the output of the SNMP traps to adhere to another MIB.

- 1 Use SSH to log in to Extreme Security as the root user.
- 2 Go to the `/opt/qradar/conf` directory and make backup copies of the following files:
  - `eventCRE.snmp.xml`
  - `offenseCRE.snmp.xml`
- 3 Open the configuration file for editing.
  - To edit the SNMP parameters for event rules, open the `eventCRE.snmp.xml` file.
  - To edit the SNMP parameters for offense rules, open the `offenseCRE.snmp.xml` file.
- 4 To change the trap that is used for SNMP trap notification, update the following text with the appropriate trap object identifier (OID):

```

-<creSNMPTrap version="3" OID="1.3.6.1.4.1.20212.1.1"
name="eventCRENotification">

```

- 5 Use the following table to help you update the variable binding information:  
Each variable binding associates a particular MIB object instance with its current value.

**Table 76: Value types for variable binding**

Value type	Description	Example
<b>string</b>	Alphanumeric characters You can configure multiple values.	
<b>integer32</b>	A numerical value	name="ATTACKER_PORT" type="integer32">%ATTACKER_PORT%
<b>oid</b>	Each SNMP trap carries an identifier that is assigned to an object within the MIB	OID="1.3.6.1.4.1.20212.2.46"
<b>gauge32</b>	A numerical value range	
<b>counter64</b>	A numerical value that increments within a defined minimum and maximum range	

- 6 For each of the value types, include any of the following fields:

**Table 77: Fields for the variable bindings**

Field	Description	Example
<b>Native</b>	For more information about these fields, see the <code>/opt/qradar/conf/snmp.help</code> file.	<b>Example</b> <sup>1</sup> If the value type is <code>ipAddress</code> , you must use a variable that is an IP address. The string value type accepts any format.
<b>Custom</b>	Custom SNMP trap information that you configured for the custom rules wizard	<b>Example</b> <sup>1</sup> If you used the default file information and want to include this information in the SNMP trap, include the following code:  <pre>&lt;variableBinding name="My Color Variable Binding" OID="1.3.6.1.4.1.20212.3.1" type="string"&gt; My favorite color is %MyColor%&lt;/variableBinding&gt;</pre>
<sup>1</sup> Surround the field name with percentage (%) signs. Within the percentage signs, fields must match the value type.		

- 7 Save and close the file.
- 8 Copy the file from the `/opt/qradar/conf` directory to the `/store/configservices/staging/globalconfig` directory.
- 9 Log in to the Extreme Security interface.
- 10 On the **Admin** tab, select **Advanced > Deploy Full Configuration**.

When you deploy the full configuration, Extreme Security restarts all services. Data collection for events stops until the deployment completes.

## Adding a custom SNMP trap to Extreme Security

In Extreme Networks Security Analytics products, you can create a new option for the SNMP trap selection in the custom rules wizard. The trap names that are specified in the list box are configured in the `snmp-master.xml` configuration file.

- 1 Use SSH to log in to Extreme Security as the root user.
- 2 Go to the `/opt/qradar/conf` directory.
- 3 Create an SNMP settings file for the new trap.



### Tip

Copy, rename, and modify one of the existing SNMP settings files.

- 4 Make a backup copy of the `snmp-master.xml` file.
- 5 Open the `snmp-master.xml` file for editing.
- 6 Add a new `<include>` element.

The `<include>` element has the following attributes:

**Table 78: Attributes for the `<include>` element**

Attribute	Description
<code>name</code>	Displayed in the list box
<code>uri</code>	The name of the custom SNMP settings file

### Example

```
<include name="Custom_Event_Name" uri="customSNMPdef01.xml" />
```

The traps are displayed in the menu in the same order in which they are listed in the `snmp-master.xml` file.

- 7 Save and close the file.
- 8 Copy the file from the `/opt/qradar/conf` directory to the `/store/configservices/staging/globalconfig` directory.
- 9 Log in to the Extreme Security interface.
- 10 On the **Admin** tab, select **Advanced > Deploy Full Configuration**.

When you deploy the full configuration, Extreme Security restarts all services. Data collection for events stops until the deployment completes.

## Sending SNMP traps to a specific host

By default, in Extreme Networks Security Analytics products, SNMP traps are sent to the host that is identified in your `host.conf` file. You can customize the `snmp.xml` file to send SNMP traps to a different host.

- 1 Use SSH to log in to Extreme Security as the root user.

- 2 Go to the `/opt/qradar/conf` directory and make backup copies of the following files:
  - `eventCRE.snmp.xml`
  - `offenseCRE.snmp.xml`
- 3 Open the configuration file for editing.
  - To edit the SNMP parameters for event rules, open the `eventCRE.snmp.xml` file.
  - To edit the SNMP parameters for offense rules, open the `offenseCRE.snmp.xml` file.
- 4 Add no more than one `<trapConfig>` element inside the `<snmp>` element inside the `<creSNMPTrap>` element and before any other child elements.

```
<trapConfig>
 <!-- All attribute values are default -->
 <snmpHost snmpVersion="3" port="162" retries="2"
timeout="500">HOST
 </snmpHost>
 <!-- Community String for Version 2 -->
 <communityString>COMMUNITY_STRING</communityString>
 <!-- authenticationProtocol (MD5 or SHA)securityLevel (AUTH_PRIV,
AUTH_NOPRIV
or NOAUTH_PRIV) -->
 <authentication
authenticationProtocol="MD5"securityLevel="AUTH_PRIV">
 AUTH_PASSWORD
 </authentication>
 <!-- decryptionProtocol (DES, AES128, AES192 or AES256) -->
 <decryption decryptionProtocol="AES256">
 DECRYPTIONPASSWORD
 </decryption>
 <!-- SNMP USER-->
 <user> SNMP_USER </user>
</trapConfig>
```

- 5 Use the following table to help you update the attributes.

**Table 79: Attribute values to update in the `<trapConfig>` element**

Element	Description
<code>&lt;/snmpHost&gt;</code>	The new host to which you want to send SNMP traps. The value for the <code>snmpVersion</code> attribute for <code>&lt;snmpHost&gt;</code> element must be 2 or 3.
<code>&lt;communityString&gt;</code>	The community string for the host
<code>&lt;authentication&gt;</code>	An authentication protocol, security level, and password for the host.
<code>&lt;decryption&gt;</code>	The decryption protocol and password for the host.
<code>&lt;user&gt;</code>	SNMP user

- 6 Save and close the file.
- 7 Log in to the Extreme Security interface.
- 8 On the **Admin** tab, select **Advanced > Deploy Full Configuration**.

When you deploy the full configuration, Extreme Security restarts all services. Data collection for events stops until the deployment completes.

# 17 Data obfuscation

Generating a private/public key pair

Configuring data obfuscation

Decrypting obfuscated data

Extreme Security asset profile data does not display obfuscated data after upgrade

To prevent unauthorized access to sensitive or user identifiable information, data obfuscation encrypts sensitive event data.

Any information from the event payload, such as user name, card number, or host name fields can be obfuscated. Use data obfuscation to help meet regulatory commission requirements and corporate privacy policies.



## Note

You cannot obfuscate a normalized numeric field, such as port or an IP address.

To configure and manage obfuscated data, do the following tasks:

- 1 Generate an RSA private/public key pair.

The obfuscation process requires that you create a public and private key for your Extreme Security Console.

Unauthorized users that attempt to query the Ariel database directly cannot view sensitive data without using the public and private decryption key.

The public key remains on the Extreme Security Console and you must store the private key in a secure location. The private key contains the decryption key that is required for administrators to view the unobfuscated data.

The `obfuscation_updater.sh` script installs the public key on your system and configures regular expression (regex) statements. The regex statements define the parameters that you want masked.

- 2 Configure data obfuscation.

Data obfuscation encrypts new events as they are processed and normalized by Extreme Security. The obfuscation process evaluates the obfuscation expression and verifies that the raw event and normalized event contain the data that is required to **mask** the data. The data that is defined in the obfuscation expression is matched to the event data, encrypted, and then written to the Ariel database.

The `obfuscation_expressions.xml` file specifies regular expression (regex) statements that identify the data that you want to obfuscate. Any text within an event that matches the regular

expressions that are specified in the `obfuscation_expressions.xml` is encrypted in both the event payload and normalized fields

- 3 When required, decrypt data obfuscation.

When suspicious activity occurs on your network, you can decrypt obfuscated data so that you can investigate all data that is involved in the activity.

The `obfuscation_decoder.sh` script decrypts the specific encrypted value that you want to investigate.

## Generating a private/public key pair

Data obfuscation and decryption requires an RSA private/public key pair.

- 1 Using SSH, log in to your Extreme Security Console as the root user.
- 2 To generate an RSA private key, type the following command:

```
openssl genrsa [-out filename] [numbits]
```

The following table describes the command options.

**Table 80: Command options for generating the RSA private key**

Option	Description
<code>[-out filename]</code>	The file name of the RSA private key file
<code>[numbits]</code>	Specifies the size, in bits, of the private key The default size is 512.

### Example

The following command generates a private key named `mykey.pem`. The size of the private key is 512 bits.

```
openssl genrsa -out mykey.pem 512
```

- 3 To format the private key, type the following command:

```
openssl pkcs8 [-topk8] [-inform PEM] [-outform PEM] [-in filename] [-out filename] [-nocrypt]
```

The following table describes the command options.

**Table 81: Options to format the private key**

Option	Description
<code>[-topk8]</code>	Reads a traditional format private key and writes the private key in PKCS #8 format
<code>[-inform]</code>	The input format of the private key as Privacy Enhanced Mail (.PEM)
<p><b>Example</b></p> <pre>-inform PEM</pre>	



**Table 81: Options to format the private key (continued)**

Option	Description
<code>[-outform]</code>	The format of the private key output as <code>.PEM</code>  Example <code>-outform PEM</code>
<code>[-in filename]</code>	The file name for the private key
<code>[-outfilename]</code>	The output file name
<code>[-nocrypt]</code>	Specifies that the private key uses the unencrypted <b>PrivateKeyInfo</b> format.

**Example**

The following command writes the private key in PKCS #8 format and uses PEM input format. The private key is output in PEM format, is named `mykey.pem`, and uses an unencrypted format.

```
openssl pkcs8 -topk8 -inform PEM -outform PEM -in mykey.pem -out
private_key.pem -nocrypt
```

- 4 To generate the RSA public key, type the following command:

```
openssl rsa [-in filename] [-pubout] [-outform DER] [-out filename]
```

The following table describes the command options

**Table 82: Command options for generating the public key**

Option	Description
<code>[-in filename]</code>	Specifies the input file name
<code>[-pubout]</code>	Generates a public key
<code>[-outform DER]</code>	The type of the public key file as DER Encoded X509 Certificate file (.DER)
<code>[-out filename]</code>	The public key file name

**Example**

In this example, the following keys are generated:

- `mykey.pem`
- `private_key.pem`
- `public_key.der`

```
openssl rsa -in mykey.pem -pubout -outform DER -out public_key.der
```

- 5 Delete the `mykey.pem` file from your system.

- 6 To install the public key, type the following command:

```
obfuscation_updater.sh [-k filename]
```

`[-k filename]` specifies the file name for the public key file that you want to install.

#### Example

The following command installs the public key named `public_key.der`.

```
obfuscation_updater.sh -k public_key.der
```



#### Note

Only one public key can be installed for each system. After you install a public key, the key cannot be overwritten.

After you install the public key on your Extreme Security Console, the Extreme Security Console ensures that the managed hosts obfuscate the data to match your obfuscation expression patterns.

To avoid unauthorized access to the obfuscated data, remove the private key file from your system. Store it in a secure location and create a backup of the private key. Follow local regulations for storage of the private key.

## Configuring data obfuscation

Use the `obfuscation_updater.sh` script to set up and configure data obfuscation.

#### Note



Events that are in the `/store` directory before you enable data obfuscation remain in their current state.

Any log source extensions that change the format of the event payload can cause issues with data.

You cannot obfuscate a normalized numeric field, such as port or an IP address.

- 1 Using SSH, log in to your Extreme Security Console as the root user:
- 2 To configure data obfuscation, type the following command:

You can run the `obfuscation_updater.sh` script from any directory on your Extreme Security Console.

```
obfuscation_updater.sh [-p filename] [-e filename]
```

`[-p filename]` specifies the private key input file name.

`[-e filename]` specifies the obfuscation expression XML input file name.

#### Example

The following command uses a file named `private_key.pem` as the private key and a file named `obfuscation_expressions.xml` as the obfuscation expression file.

```
obfuscation_updater.sh -p private_key.pem -e
obfuscation_expressions.xml
```

- 3 Configure the attributes of the `obfuscation_expressions.xml` file.

The `obfuscation_expressions.xml` file defines the regular expressions that are used to obfuscate data. You can add multiple regular expressions.

The following table describes the `obfuscation_expressions.xml` file attributes that you can configure.

**Table 83: Attributes of the `obfuscation_expressions.xml` file**

Attributes	Description	Database table that contains the attribute value
<expression name>	A unique name to identify the regular expression	
<regex>	The regular expression that you want to use to extract the data for obfuscation	
<captureGroup>	The capture group that is associated with the regular expression	
<deviceTypeId>	Identifies the <i>Log Source</i> type. Identifies the event and extract the data to be obfuscated.	<sup>1</sup> <i>sensordeviceType</i>
<deviceId>	Identifies the <i>Log Source</i> . Identifies the event and extract the data to be obfuscated.	<sup>1</sup> <i>sensordevice</i>
<qidId>	Identifies the <i>Event</i> name. Identifies the event and extract the data to obfuscate.	<sup>1</sup> <i>qidmap</i>
<category>	Identifies the low-level <i>Category of the Event</i> . Identifies the event and extract the data to be obfuscated.	<sup>1</sup> <i>Type</i>
<enabled>	If true, enables the regular expression. If false, disables the regular expression.	
<sup>1</sup> You can configure a value of <b>-1</b> to disable this attribute.		

## Examples of data obfuscation

- 1 The following code shows an example of event payload.

```
LEEF:1.0|VMware|EMC VMware|5.1 Tue Oct 09 12:39:31 EDT
2012|jobEnable| usrName=john.smith msg=john.smith@1.1.1.1
src=1.1.1.1
```

- 2 The following code shows an example of an `obfuscation_expressions.xml` file.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ObfuscationExpressions>
 <expression name="VMwareUsers">
 <regex>user (\S+)</regex>
 <deviceTypeId>-1</deviceTypeId>
```

```

 <deviceId>-1</deviceId>
 <qidId>-1</qidId>
 <category>-1</category>
 <enabled>true</enabled>
 </expression>

 <expression name="VMwarehosts">
 <regex>ruser=(\S+)</regex>
 <deviceId>-1</deviceId>
 <qidId>-1</qidId>
 <category>-1</category>
 <enabled>>false</enabled>
 </expression>
</ObfuscationExpressions>

```

- The following example shows the regular expressions that can parse user names.

**Table 84: Example regex patterns that can parse user names**

Example regex patterns	Matches
<code>usrName=([0-9a-zA-Z]([-\.\w]*[0-9a-zA-Z]))*@[0-9a-zA-Z]([-\w]*[0-9a-zA-Z]\.)+[a-zA-Z]{2,20})\$</code>	john_smith@IBM.com, jon@ibm.com, jon@us.ibm.com
<code>usrName=(^[[\w]+[^\W])([^\W]\.?)([\w]+[^\W]\$))</code>	john.smith, John.Smith, john, jon_smith
<code>usrName=^([a-zA-Z])[a-zA-Z_-]*[\w_-]*[\S\$] ^([a-zA-Z])[0-9_-]*[\S\$] ^[a-zA-Z]*[\S]\$</code>	johnsmith, Johnsmith123, john_smith123, john123_smith, john-smith
<code>usrName=(/S+)</code>	Matches any non-white space after the equal, =, sign. This greedy regular expression can lead to system performance issues.
<code>msg=([0-9a-zA-Z]([-\.\w]*[0-9a-zA-Z]))*\b((01)?\d?\d 2[0-4]\d 25[0-5])\.\.){3}((01)?\d?\d 2[0-4]\d 25[0-5])\b</code>	Matches users with IP address.  <b>Example</b> john.smith@1.1.1.1
<code>src=\b((01)?\d?\d 2[0-4]\d 25[0-5])\.\.){3}((01)?\d?\d 2[0-4]\d 25[0-5])\b</code>	Matches IP address formats.
<code>host=^(([a-zA-Z0-9] [a-zA-Z0-9][a-zA-Z0-9\_-]*[a-zA-Z0-9])\.)*([A-Za-z0-9] [A-Za-z0-9][A-Za-z0-9\_-]*[A-Za-z0-9])\$</code>	hostname.ibm.com, hostname.co.uk,

## Decrypting obfuscated data

When data obfuscation is configured on an Extreme Networks Security Analytics system, the encrypted version of the data is displayed in the columns and parameters on the user interface. Use the `obfuscation_decoder.sh` script to decrypt obfuscated data.

- Log in to the Extreme Networks Security Analytics user interface and copy the obfuscated text that you want to decrypt.

- Using SSH, log in to your Extreme Security Console as the root user.

User name: `root`

- Create a directory and copy the public and private keys to this directory.
- Go to the directory where the keys are located.
- To decrypt the obfuscated text, type the following command:

```
obfuscation_decoder.sh -k publickey filename -p privatekey filename -d
<obfuscated_text>
```

The following table describes the `obfuscation_decoder.sh` options.

**Table 85: Options for the `obfuscation_decoder.sh` script**

Option	Description
<code>-k <b>publickey</b> filename</code>	The public key file name
<code>-p <b>privatekey</b> filename</code>	The private key file name
<code>-d <b>obfuscated</b> text</code>	The obfuscated text that you want to decrypt

#### Example

The following command decrypts the masked data.

```
obfuscation_decoder.sh -k public_key.der -p private_key.pem -d
obfuscated_text
```

## Extreme Security asset profile data does not display obfuscated data after upgrade

User names and host name data that are part of the Extreme Networks Security Analytics asset profile before your upgrade to Extreme Security V7.2 might not display obfuscated data as expected.

To obfuscate asset profile data, follow these steps:

- Log in to the Extreme Security Console.
- Click the **Assets** tab.
- To remove unobfuscated hosts and user names, click **Actions > Delete Listed**.
- Run scan profile manually or run schedule the scan profile to run.
- To repopulate the data for building blocks on your Extreme Security system, run the **Server Discovery** tool.

# 18 Audit logs

## Viewing the audit log file Logged actions

Changes that are made by Extreme Security users are recorded in the audit logs.

You can view the audit logs to monitor changes to Extreme Security and the users who change settings.

All audit logs are stored in plain text and are archived and compressed when the audit log file reaches 200 MB. The current log file is named `audit.log`. When the file reaches 200 MB, the file is compressed and renamed to `audit.1.gz`, `audit.2.gz`. The file number increments each time that a log file is archived. Extreme Security stores up to 50 archived log files.

## Viewing the audit log file

Use Secure Shell (SSH) to log in to your Extreme Security system and monitor changes to your system.

You can use **Log Activity** tab to view normalized audit log events.

The maximum size of any audit message, excluding date, time, and host name, is 1024 characters.

Each entry in the log file displays by using the following format:

```
<date_time> <host_name> <user>@<IP address> (thread ID) [<category>]
[<sub-category>] [<action>] <payload>
```

The following table describes the log file format options.

**Table 86: Description of the parts of the log file format**

File format part	Description
<code>date_time</code>	The date and time of the activity in the format: Month Date HH:MM:SS
<code>host_name</code>	The host name of the Console where this activity was logged.
<code>user</code>	The name of the user who changed the settings.
<code>IP address</code>	The IP address of the user who changed the settings.
<code>thread ID)</code>	The identifier of the Java™ thread that logged this activity.
<code>category</code>	The high-level category of this activity.
<code>sub-categor</code>	The low-level category of this activity.

**Table 86: Description of the parts of the log file format (continued)**

File format part	Description
<i>action</i>	The activity that occurred.
<i>payload</i>	The complete record, which might include the user record or event rule, that changed.

1 Using SSH, log in to Extreme Security as the root user:

2 **User Name:** `root`

3 **Password:** `password`

4 Go to the following directory:

`/var/log/audit`

5 Open and view the audit log file.

## Logged actions

Understand the content of Extreme Security audit log file in the `/var/log/audit` directory. The audit log file contains logged actions.

The following list describes the categories of actions that are in the audit log file:

<b>Administrator Authentication</b>	<ul style="list-style-type: none"> <li>Log in to the Administration Console</li> <li>Log out of the Administration Console.</li> </ul>
<b>Assets</b>	<ul style="list-style-type: none"> <li>Delete an asset.</li> <li>Delete all assets.</li> </ul>
<b>Audit Log Access</b>	A search that includes events that have a high-level event category of Audit.
<b>Backup and Recovery</b>	<ul style="list-style-type: none"> <li>Edit the configuration.</li> <li>Initiate the backup.</li> <li>Complete the backup.</li> <li>Fail the backup.</li> <li>Delete the backup.</li> <li>Synchronize the backup.</li> <li>Cancel the backup.</li> <li>Initiate the restore.</li> <li>Upload a backup.</li> <li>Upload an invalid backup.</li> <li>Initiate the restore.</li> <li>Purge the backup.</li> </ul>
<b>Custom Properties</b>	<ul style="list-style-type: none"> <li>Add a custom event property.</li> <li>Edit a custom event property.</li> <li>Delete a custom event property.</li> </ul>
<b>Chart Configuration</b>	Save event chart configuration.
<b>Custom Property Expressions</b>	<ul style="list-style-type: none"> <li>Add a custom event property expression.</li> <li>Edit a custom event property expression.</li> <li>Delete a custom event property expression.</li> </ul>

Retention Buckets	<ul style="list-style-type: none"><li>• Add a bucket.</li><li>• Delete a bucket.</li><li>• Edit a bucket.</li><li>• Enable or disable a bucket.</li></ul>
Groups	<ul style="list-style-type: none"><li>• Add a group.</li><li>• Delete a group.</li><li>• Edit a group.</li></ul>
High Availability	<ul style="list-style-type: none"><li>• Add a license key.</li><li>• Revert a license.</li><li>• Delete a license key.</li></ul>
Log Source Extension	<ul style="list-style-type: none"><li>• Add an log source extension.</li><li>• Edit the log source extension.</li><li>• Delete a log source extension.</li><li>• Upload a log source extension.</li><li>• Upload a log source extension successfully.</li><li>• Upload an invalid log source extension.</li><li>• Download a log source extension.</li><li>• Report a log source extension.</li><li>• Modify a log sources association to a device or device type.</li></ul>
Protocol Configuration	<ul style="list-style-type: none"><li>• Add a protocol configuration.</li><li>• Delete a protocol configuration.</li><li>• Edit a protocol configuration.</li></ul>
QIDmap	<ul style="list-style-type: none"><li>• Add a QID map entry.</li><li>• Edit a QID map entry.</li></ul>
Vulnerability Manager	<ul style="list-style-type: none"><li>• Create a scanner schedule.</li><li>• Update a scanner schedule.</li><li>• Delete a scanner schedule.</li><li>• Start a scanner schedule.</li><li>• Pause a scanner schedule.</li><li>• Resume a scanner schedule.</li></ul>
Reference Sets	<ul style="list-style-type: none"><li>• Create a reference set.</li><li>• Edit a reference set.</li><li>• Purge elements in a reference set.</li><li>• Delete a reference set.</li><li>• Add reference set elements.</li><li>• Delete reference set elements.</li><li>• Delete all reference set elements.</li><li>• Import reference set elements.</li><li>• Export reference set elements.</li></ul>
Reports	<ul style="list-style-type: none"><li>• Add a template.</li><li>• Delete a template.</li><li>• Edit a template.</li><li>• Generate a report.</li><li>• Delete a report.</li></ul>



	<ul style="list-style-type: none"><li>• Delete generated content.</li><li>• View a generated report.</li><li>• Email a generated report.</li></ul>
Root Login	<ul style="list-style-type: none"><li>• Log in to Extreme Security, as root.</li><li>• Log out of Extreme Security, as root.</li></ul>
Rules	<ul style="list-style-type: none"><li>• Add a rule.</li><li>• Delete a rule.</li><li>• Edit a rule.</li></ul>
Scanner Schedule	<ul style="list-style-type: none"><li>• Add a schedule.</li><li>• Edit a schedule.</li><li>• Delete a schedule.</li></ul>
Session Authentication	<ul style="list-style-type: none"><li>• Create an administration session.</li><li>• Terminate an administration session.</li><li>• Deny an invalid authentication session.</li><li>• Expire a session authentication.</li><li>• Create an authentication session.</li><li>• Terminate an authentication session</li></ul>
Store and Forward	<ul style="list-style-type: none"><li>• Add a Store and Forward schedule.</li><li>• Edit a Store and Forward schedule.</li><li>• Delete a Store and Forward schedule.</li></ul>
Syslog Forwarding	<ul style="list-style-type: none"><li>• Add a syslog forwarding.</li><li>• Delete a syslog forwarding.</li><li>• Edit a syslog forwarding.</li></ul>
System Management	<ul style="list-style-type: none"><li>• Shut down a system.</li><li>• Restart a system.</li></ul>
User Accounts	<ul style="list-style-type: none"><li>• Add an account.</li><li>• Edit an account.</li><li>• Delete an account.</li></ul>
User Authentication	<ul style="list-style-type: none"><li>• Log in to the user interface.</li><li>• Log out of the user interface.</li></ul>
User Authentication Ariel	<ul style="list-style-type: none"><li>• Deny a login attempt.</li><li>• Add an Ariel property.</li><li>• Delete an Ariel property.</li><li>• Edit an Ariel property.</li><li>• Add an Ariel property extension.</li><li>• Delete an Ariel property extension.</li><li>• Edit an Ariel property extension.</li></ul>
User Roles	<ul style="list-style-type: none"><li>• Add a role.</li><li>• Edit a role.</li><li>• Delete a role.</li></ul>

# 19 Event categories

## High-level event categories

Recon  
DoS  
Authentication  
Access  
Exploit  
Malware  
Suspicious Activity  
System  
Policy  
Unknown  
CRE  
Potential Exploit  
User Defined  
SIM Audit  
VIS Host Discovery  
Application  
Audit  
Risk  
Risk Manager Audit  
Control  
Asset Profiler

Event categories are used to group incoming events for processing by Extreme Networks Security Analytics. The event categories are searchable and help you monitor your network.

Events that occur on your network are aggregated into high-level and low-level categories. Each high-level category contains low-level categories and an associated severity level. You can review the severity levels that are assigned to events and adjust them to suit your corporate policy needs.

## High-level event categories

Events in Extreme Security log sources are grouped into high-level categories. Each event is assigned to a specific high-level category.

Categorizing the incoming events ensures that you can easily search the data..

The following table describes the high-level event categories.

**Table 87: High-level event categories**

Category	Description
<b>Recon</b> on page 195	Events that are related to scanning and other techniques that are used to identify network resources, for example, network or host port scans.
<b>DoS</b> on page 196	Events that are related to denial-of-service (DoS) or distributed denial-of-service (DDoS) attacks against services or hosts, for example, brute force network DoS attacks.
<b>Authentication</b> on page 199	Events that are related to authentication controls, group, or privilege change, for example, log in or log out.
<b>Access</b> on page 203	Events resulting from an attempt to access network resources, for example, firewall accept or deny.
<b>Exploit</b> on page 205	Events that are related to application exploits and buffer overflow attempts, for example, buffer overflow or web application exploits.
<b>Malware</b> on page 206	Events that are related to viruses, trojans, back door attacks, or other forms of hostile software. Malware events might include a virus, trojan, malicious software, or spyware.
<b>Suspicious Activity</b> on page 207	The nature of the threat is unknown but behavior is suspicious. The threat might include protocol anomalies that potentially indicate evasive techniques, for example, packet fragmentation or known intrusion detection system (IDS) evasion techniques.
<b>System</b> on page 209	Events that are related to system changes, software installation, or status messages.
<b>Policy</b> on page 212	Events regarding corporate policy violations or misuse.
<b>Unknown</b> on page 213	Events that are related to unknown activity on your system.
<b>CRE</b> on page 214	Events that are generated from an event rule.
<b>Potential Exploit</b> on page 214	Events relate to potential application exploits and buffer overflow attempts.
<b>User Defined</b> on page 215	Events that are related to user-defined objects.
<b>SIM Audit</b> on page 216	Events that are related to user interaction with the Console and administrative functions.
<b>Application</b> on page 218	Events that are related to application activity.
<b>Audit</b> on page 232	Events that are related to audit activity.
<b>Control</b> on page 234	Events that are related to your hardware system.
<b>Asset Profiler</b> on page 236	Events that are related to asset profiles.

## Recon

The Recon category contains events that are related to scanning and other techniques that are used to identify network resources.

The following table describes the low-level event categories and associated severity levels for the Recon category.

**Table 88: Low-level categories and severity levels for the Recon events category**

Low-level event category	Description	Severity level (0 - 10)
Unknown Form of Recon	An unknown form of reconnaissance.	2
Application Query	Reconnaissance to applications on your system.	3
Host Query	Reconnaissance to a host in your network.	3
Network Sweep	Reconnaissance on your network.	4
Mail Reconnaissance	Reconnaissance on your mail system.	3
Windows™ Reconnaissance	Reconnaissance for Windows operating system.	3
Portmap / RPC r\request	Reconnaissance on your portmap or RPC request.	3
Host Port Scan	Indicates that a scan occurred on the host ports.	4
RPC Dump	Indicates that Remote Procedure Call (RPC) information is removed.	3
DNS Reconnaissance	Reconnaissance on the DNS server.	3
Misc Reconnaissance Event	Miscellaneous reconnaissance event.	2
Web Reconnaissance	Web reconnaissance on your network.	3
Database Reconnaissance	Database reconnaissance on your network.	3
ICMP Reconnaissance	Reconnaissance on ICMP traffic.	3
UDP Reconnaissance	Reconnaissance on UDP traffic.	3
SNMP Reconnaissance	Reconnaissance on SNMP traffic.	3
ICMP Host Query	Indicates an ICMP host query.	3
UDP Host Query	Indicates a UDP host query.	3
NMAP Reconnaissance	Indicates NMAP reconnaissance.	3
TCP Reconnaissance	Indicates TCP reconnaissance on your network.	3
UNIX Reconnaissance	Reconnaissance on your UNIX™ network.	3
FTP Reconnaissance	Indicates FTP reconnaissance.	3

## DoS

The DoS category contains events that are related to denial-of-service (DoS) attacks against services or hosts.

The following table describes the low-level event categories and associated severity levels for the DoS category.

**Table 89: Low-level categories and severity levels for the DoS events category**

Low-level event category	Description	Severity level (0 - 10)
Unknown DoS Attack	Indicates an unknown DoS attack.	8
ICMP DoS	Indicates an ICMP DoS attack.	9

**Table 89: Low-level categories and severity levels for the DoS events category (continued)**

Low-level event category	Description	Severity level (0 - 10)
TCP DoS	Indicates a TCP DoS attack.	9
UDP DoS	Indicates a UDP DoS attack.	9
DNS Service DoS	Indicates a DNS service DoS attack.	8
Web Service DoS	Indicates a web service DoS attack.	8
Mail Service DoS	Indicates a mail server DoS attack.	8
Distributed DoS	Indicates a distributed DoS attack.	9
Misc DoS	Indicates a miscellaneous DoS attack.	8
UNIX™ DoS	Indicates a UNIX™ DoS attack.	8
Windows™ DoS	Indicates a Windows™ DoS attack.	8
Database DoS	Indicates a database DoS attack.	8
FTP DoS	Indicates an FTP DoS attack.	8
Infrastructure DoS	Indicates a DoS attack on the infrastructure.	8
Telnet DoS	Indicates a Telnet DoS attack.	8
Brute Force Login	Indicates access to your system through unauthorized methods.	8
High Rate TCP DoS	Indicates a high rate TCP DoS attack.	8
High Rate UDP DoS	Indicates a high rate UDP DoS attack.	8
High Rate ICMP DoS	Indicates a high rate ICMP DoS attack.	8
High Rate DoS	Indicates a high rate DoS attack.	8
Medium Rate TCP DoS	Indicates a medium rate TCP attack.	8
Medium Rate UDP DoS	Indicates a medium rate UDP attack.	8
Medium Rate ICMP DoS	Indicates a medium rate ICMP attack.	8
Medium Rate DoS	Indicates a medium rate DoS attack.	8
Medium Rate DoS	Indicates a medium rate DoS attack.	8
Low Rate TCP DoS	Indicates a low rate TCP DoS attack.	8
Low Rate UDP DoS	Indicates a low rate UDP DoS attack.	8
Low Rate ICMP DoS	Indicates a low rate ICMP DoS attack.	8
Low Rate DoS	Indicates a low rate DoS attack.	8
Distributed High Rate TCP DoS	Indicates a distributed high rate TCP DoS attack.	8
Distributed High Rate UDP DoS	Indicates a distributed high rate UDP DoS attack.	8
Distributed High Rate ICMP DoS	Indicates a distributed high rate ICMP DoS attack.	8
Distributed High Rate DoS	Indicates a distributed high rate DoS attack.	8
Distributed Medium Rate TCP DoS	Indicates a distributed medium rate TCP DoS attack.	8

**Table 89: Low-level categories and severity levels for the DoS events category (continued)**

Low-level event category	Description	Severity level (0 - 10)
Distributed Medium Rate UDP DoS	Indicates a distributed medium rate UDP DoS attack.	8
Distributed Medium Rate ICMP DoS	Indicates a distributed medium rate ICMP DoS attack.	8
Distributed Medium Rate DoS	Indicates a distributed medium rate DoS attack.	8
Distributed Low Rate TCP DoS	Indicates a distributed low rate TCP DoS attack.	8
Distributed Low Rate UDP DoS	Indicates a distributed low rate UDP DoS attack.	8
Distributed Low Rate ICMP DoS	Indicates a distributed low rate ICMP DoS attack.	8
Distributed Low Rate DoS	Indicates a distributed low rate DoS attack.	8
High Rate TCP Scan	Indicates a high rate TCP scan.	8
High Rate UDP Scan	Indicates a high rate UDP scan.	8
High Rate ICMP Scan	Indicates a high rate ICMP scan.	8
High Rate Scan	Indicates a high rate scan.	8
Medium Rate TCP Scan	Indicates a medium rate TCP scan.	8
Medium Rate UDP Scan	Indicates a medium rate UDP scan.	8
Medium Rate ICMP Scan	Indicates a medium rate ICMP scan.	8
Medium Rate Scan	Indicates a medium rate scan.	8
Low Rate TCP Scan	Indicates a low rate TCP scan.	8
Low Rate UDP Scan	Indicates a low rate UDP scan.	8
Low Rate ICMP Scan	Indicates a low rate ICMP scan.	8
Low Rate Scan	Indicates a low rate scan.	8
VoIP DoS	Indicates a VoIP DoS attack.	8
Flood	Indicates a Flood attack.	8
TCP Flood	Indicates a TCP flood attack.	8
UDP Flood	Indicates a UDP flood attack.	8
ICMP Flood	Indicates an ICMP flood attack.	8
SYN Flood	Indicates a SYN flood attack.	8
URG Flood	Indicates a flood attack with the urgent (URG) flag on.	8
SYN URG Flood	Indicates a SYN flood attack with the urgent (URG) flag on.	8
SYN FIN Flood	Indicates a SYN FIN flood attack.	8
SYN ACK Flood	Indicates a SYN ACK flood attack.	8

## Authentication

The authentication category contains events that are related to authentication, sessions, and access controls that monitor users on the network.

The following table describes the low-level event categories and associated severity levels for the authentication category.

**Table 90: Low-level categories and severity levels for the authentication events category**

Low-level event category	Description	Severity level (0 - 10)
Unknown Authentication	Indicates unknown authentication.	1
Host Login Succeeded	Indicates a successful host login.	1
Host Login Failed	Indicates that the host login failed.	3
Misc Login Succeeded	Indicates that the login sequence succeeded.	1
Misc Login Failed	Indicates that login sequence failed.	3
Privilege Escalation Failed	Indicates that the privileged escalation failed.	3
Privilege Escalation Succeeded	Indicates that the privilege escalation succeeded.	1
Mail Service Login Succeeded	Indicates that the mail service login succeeded.	1
Mail Service Login Failed	Indicates that the mail service login failed.	3
Auth Server Login Failed	Indicates that the authentication server login failed.	3
Auth Server Login Succeeded	Indicates that the authentication server login succeeded.	1
Web Service Login Succeeded	Indicates that the web service login succeeded.	1
Web Service Login Failed	Indicates that the web service login failed.	3
Admin Login Successful	Indicates that an administrative login was successful.	1
Admin Login Failure	Indicates the administrative login failed.	3
Suspicious Username	Indicates that a user attempted to access the network by using an incorrect user name.	4
Login with username/ password defaults successful	Indicates that a user accessed the network by using the default user name and password.	4
Login with username/ password defaults failed	Indicates that a user was unsuccessful accessing the network by using the default user name and password.	4
FTP Login Succeeded	Indicates that the FTP login was successful.	1
FTP Login Failed	Indicates that the FTP login failed.	3
SSH Login Succeeded	Indicates that the SSH login was successful.	1
SSH Login Failed	Indicates that the SSH login failed.	2
User Right Assigned	Indicates that user access to network resources was successfully granted.	1
User Right Removed	Indicates that user access to network resources was successfully removed.	1

**Table 90: Low-level categories and severity levels for the authentication events category (continued)**

Low-level event category	Description	Severity level (0 - 10)
Trusted Domain Added	Indicates that a trusted domain was successfully added to your deployment.	1
Trusted Domain Removed	Indicates that a trusted domain was removed from your deployment.	1
System Security Access Granted	Indicates that system security access was successfully granted.	1
System Security Access Removed	Indicates that system security access was successfully removed.	1
Policy Added	Indicates that a policy was successfully added.	1
Policy Change	Indicates that a policy was successfully changed.	1
User Account Added	Indicates that a user account was successfully added.	1
User Account Changed	Indicates a change to an existing user account.	1
Password Change Failed	Indicates that an attempt to change an existing password failed.	3
Password Change Succeeded	Indicates that a password change was successful.	1
User Account Removed	Indicates that a user account was successfully removed.	1
Group Member Added	Indicates that a group member was successfully added.	1
Group Member Removed	Indicates that a group member was removed.	1
Group Added	Indicates that a group was successfully added.	1
Group Changed	Indicates a change to an existing group.	1
Group Removed	Indicates that a group was removed.	1
Computer Account Added	Indicates that a computer account was successfully added.	1
Computer Account Changed	Indicates a change to an existing computer account.	1
Computer Account Removed	Indicates that a computer account was successfully removed.	1
Remote Access Login Succeeded	Indicates that access to the network by using a remote login was successful.	1
Remote Access Login Failed	Indicates that an attempt to access the network by using a remote login failed.	3
General Authentication Successful	Indicates that the authentication processes was successful.	1
General Authentication Failed	Indicates that the authentication process failed.	3
Telnet Login Succeeded	Indicates that the telnet login was successful.	1
Telnet Login Failed	Indicates that the telnet login failed.	3
Suspicious Password	Indicates that a user attempted to log in by using a suspicious password.	4
Samba Login Successful	Indicates that a user successfully logged in by using Samba.	1



**Table 90: Low-level categories and severity levels for the authentication events category (continued)**

Low-level event category	Description	Severity level (0 - 10)
Samba Login Failed	Indicates a user failed to log in by using Samba.	3
Auth Server Session Opened	Indicates that a communication session with the authentication server was started.	1
Auth Server Session Closed	Indicates that a communication session with the authentication server was closed.	1
Firewall Session Closed	Indicates that a firewall session was closed.	1
Host Logout	Indicates that a host successfully logged out.	1
Misc Logout	Indicates that a user successfully logged out.	1
Auth Server Logout	Indicates that the process to log out of the authentication server was successful.	1
Web Service Logout	Indicates that the process to log out of the web service was successful.	1
Admin Logout	Indicates that the administrative user successfully logged out.	1
FTP Logout	Indicates that the process to log out of the FTP service was successful.	1
SSH Logout	Indicates that the process to log out of the SSH session was successful.	1
Remote Access Logout	Indicates that the process to log out using remote access was successful.	1
Telnet Logout	Indicates that the process to log out of the Telnet session was successful.	1
Samba Logout	Indicates that the process to log out of Samba was successful.	1
SSH Session Started	Indicates that the SSH login session was initiated on a host.	1
SSH Session Finished	Indicates the termination of an SSH login session on a host.	1
Admin Session Started	Indicates that a login session was initiated on a host by an administrative or privileged user.	1
Admin Session Finished	Indicates the termination of an administrator or privileged users login session on a host.	1
VoIP Login Succeeded	Indicates a successful VoIP service login	1
VoIP Login Failed	Indicates an unsuccessful attempt to access VoIP service.	1
VoIP Logout	Indicates a user logout,	1
VoIP Session Initiated	Indicates the beginning of a VoIP session.	1
VoIP Session Terminated	Indicates the end of a VoIP session.	1
Database Login Succeeded	Indicates a successful database login.	1
Database Login Failure	Indicates a database login attempt failed.	3

**Table 90: Low-level categories and severity levels for the authentication events category (continued)**

Low-level event category	Description	Severity level (0 - 10)
IKE Authentication Failed	Indicates a failed Internet Key Exchange (IKE) authentication was detected.	3
IKE Authentication Succeeded	Indicates that a successful IKE authentication was detected.	1
IKE Session Started	Indicates that an IKE session started.	1
IKE Session Ended	Indicates that an IKE session ended.	1
IKE Error	Indicates an IKE error message.	1
IKE Status	Indicates IKE status message.	1
RADIUS Session Started	Indicates that a RADIUS session started.	1
RADIUS Session Ended	Indicates a RADIUS session ended.	1
RADIUS Session Denied	Indicates that a RADIUS session was denied.	1
RADIUS Session Status	Indicates a RADIUS session status message.	1
RADIUS Authentication Failed	Indicates a RADIUS authentication failure.	3
RADIUS Authentication Successful	Indicates a RADIUS authentication succeeded.	1
TACACS Session Started	Indicates a TACACS session started.	1
TACACS Session Ended	Indicates a TACACS session ended.	1
TACACS Session Denied	Indicates that a TACACS session was denied.	1
TACACS Session Status	Indicates a TACACS session status message.	1
TACACS Authentication Successful	Indicates a TACACS authentication succeeded.	1
TACACS Authentication Failed	Indicates a TACACS authentication failure.	1
Deauthenticating Host Succeeded	Indicates that the deauthentication of a host was successful.	1
Deauthenticating Host Failed	Indicates that the deauthentication of a host failed.	3
Station Authentication Succeeded	Indicates that the station authentication was successful.	1
Station Authentication Failed	Indicates that the station authentication of a host failed.	3
Station Association Succeeded	Indicates that the station association was successful.	1
Station Association Failed	Indicates that the station association failed.	3
Station Reassociation Succeeded	Indicates that the station reassociation was successful.	1
Station Reassociation Failed	Indicates that the station association failed.	3
Disassociating Host Succeeded	Indicates that the disassociating a host was successful.	1
Disassociating Host Failed	Indicates that the disassociating a host failed.	3
SA Error	Indicates a Security Association (SA) error message.	5
SA Creation Failure	Indicates a Security Association (SA) creation failure.	3

**Table 90: Low-level categories and severity levels for the authentication events category (continued)**

Low-level event category	Description	Severity level (0 - 10)
SA Established	Indicates that a Security Association (SA) connection established.	1
SA Rejected	Indicates that a Security Association (SA) connection rejected.	3
Deleting SA	Indicates the deletion of a Security Association (SA).	1
Creating SA	Indicates the creation of a Security Association (SA).	1
Certificate Mismatch	Indicates a certificate mismatch.	3
Credentials Mismatch	Indicates a credentials mismatch.	3
Admin Login Attempt	Indicates an admin login attempt.	2
User Login Attempt	Indicates a user login attempt.	2
User Login Successful	Indicates a successful user login.	1
User Login Failure	Indicates a failed user login.	3
SFTP Login Succeeded	Indicates a successful SSH File Transfer Protocol (SFTP) login.	1
SFTP Login Failed	Indicates a failed SSH File Transfer Protocol (SFTP) login.	3
SFTP Logout	Indicates an SSH File Transfer Protocol (SFTP) logout.	1

## Access

The access category contains authentication and access controls that are used for monitoring network events.

The following table describes the low-level event categories and associated severity levels for the access category.

**Table 91: Low-level categories and severity levels for the access events category**

Low-level event category	Description	Severity level (0 - 10)
Unknown Network Communication Event	Indicates an unknown network communication event.	3
Firewall Permit	Indicates that access to the firewall was allowed.	0
Firewall Deny	Indicates that access to the firewall was denied.	4
Flow Context Response (Extreme SIEM only)	Indicates events from the Classification Engine in response to a SIM request.	5
Misc Network Communication Event	Indicates a miscellaneous communications event.	3
IPS Deny	Indicates Intrusion Prevention Systems (IPS) denied traffic.	4

**Table 91: Low-level categories and severity levels for the access events category (continued)**

Low-level event category	Description	Severity level (0 - 10)
Firewall Session Opened	Indicates that the firewall session was opened.	0
Firewall Session Closed	Indicates that the firewall session was closed.	0
Dynamic Address Translation Successful	Indicates that dynamic address translation was successful.	0
No Translation Group Found	Indicates that no translation group was found.	2
Misc Authorization	Indicates that access was granted to a miscellaneous authentication server.	2
ACL Permit	Indicates that an Access Control List (ACL) allowed access.	0
ACL Deny	Indicates that an Access Control List (ACL) denied access.	4
Access Permitted	Indicates that access was allowed.	0
Access Denied	Indicates that access was denied.	4
Session Opened	Indicates that a session was opened.	1
Session Closed	Indicates that a session was closed.	1
Session Reset	Indicates that a session was reset.	3
Session Terminated	Indicates that a session was allowed.	4
Session Denied	Indicates that a session was denied.	5
Session in Progress	Indicates that a session is in progress.	1
Session Delayed	Indicates that a session was delayed.	3
Session Queued	Indicates that a session was queued.	1
Session Inbound	Indicates that a session is inbound.	1
Session Outbound	Indicates that a session is outbound.	1
Unauthorized Access Attempt	Indicates that an unauthorized access attempt was detected.	6
Misc Application Action Allowed	Indicates that an application action was allowed.	1
Misc Application Action Denied	Indicates that an application action was denied.	3
Database Action Allowed	Indicates that a database action was allowed.	1
Database Action Denied	Indicates that a database action was denied.	3
FTP Action Allowed	Indicates that an FTP action was allowed.	1
FTP Action Denied	Indicates that an FTP action was denied.	3
Object Cached	Indicates that an object was cached.	1
Object Not Cached	Indicates that an object was not cached.	1
Rate Limiting	Indicates that the network rate-limits traffic.	4
No Rate Limiting	Indicates that the network does not rate-limit traffic.	0

## Exploit

The exploit category contains events where a communication or an access exploit occurred.

The following table describes the low-level event categories and associated severity levels for the exploit category.

**Table 92: Low-level categories and severity levels for the exploit events category**

Low-level event category	Description	Severity level (0 - 10)
Unknown Exploit Attack	Indicates an unknown exploit attack.	9
Buffer Overflow	Indicates a buffer overflow.	9
DNS Exploit	Indicates a DNS exploit.	9
Telnet Exploit	Indicates a Telnet exploit.	9
Linux™ Exploit	Indicates a Linux™ exploit.	9
UNIX™ Exploit	Indicates a UNIX™ exploit.	9
Windows™ Exploit	Indicates a Microsoft™ Windows™ exploit.	9
Mail Exploit	Indicates a mail server exploit.	9
Infrastructure Exploit	Indicates an infrastructure exploit.	9
Misc Exploit	Indicates a miscellaneous exploit.	9
Web Exploit	Indicates a web exploit.	9
Session Hijack	Indicates that a session in your network was interceded.	9
Worm Active	Indicates an active worm.	10
Password Guess/Retrieve	Indicates that a user requested access to their password information from the database.	9
FTP Exploit	Indicates an FTP exploit.	9
RPC Exploit	Indicates an RPC exploit.	9
SNMP Exploit	Indicates an SNMP exploit.	9
NOOP Exploit	Indicates an NOOP exploit.	9
Samba Exploit	Indicates a Samba exploit.	9
Database Exploit	Indicates a database exploit.	9
SSH Exploit	Indicates an SSH exploit.	9
ICMP Exploit	Indicates an ICMP exploit.	9
UDP Exploit	Indicates a UDP exploit.	9
Browser Exploit	Indicates an exploit on your browser.	9
DHCP Exploit	Indicates a DHCP exploit	9
Remote Access Exploit	Indicates a remote access exploit	9
ActiveX Exploit	Indicates an exploit through an ActiveX application.	9
SQL Injection	Indicates that an SQL injection occurred.	9

**Table 92: Low-level categories and severity levels for the exploit events category (continued)**

Low-level event category	Description	Severity level (0 - 10)
Cross-Site Scripting	Indicates a cross-site scripting vulnerability.	9
Format String Vulnerability	Indicates a format string vulnerability.	9
Input Validation Exploit	Indicates that an input validation exploit attempt was detected.	9
Remote Code Execution	Indicates that a remote code execution attempt was detected.	9
Memory Corruption	Indicates that a memory corruption exploit was detected.	9
Command Execution	Indicates that a remote command execution attempt was detected.	9

## Malware

The malicious software (malware) category contains events that are related to application exploits and buffer overflow attempts.

The following table describes the low-level event categories and associated severity levels for the malware category.

**Table 93: Low-level categories and severity levels for the malware events category**

Low-level event category	Description	Severity level (0 - 10)
Unknown Malware	Indicates an unknown virus.	4
Backdoor Detected	Indicates that a back door to the system was detected.	9
Hostile Mail Attachment	Indicates a hostile mail attachment.	6
Malicious Software	Indicates a virus.	6
Hostile Software Download	Indicates a hostile software download to your network.	6
Virus Detected	Indicates that a virus was detected.	8
Misc Malware	Indicates miscellaneous malicious software	4
Trojan Detected	Indicates that a trojan was detected.	7
Spyware Detected	Indicates that spyware was detected on your system.	6
Content Scan	Indicates that an attempted scan of your content was detected.	3
Content Scan Failed	Indicates that a scan of your content failed.	8
Content Scan Successful	Indicates that a scan of your content was successful.	3
Content Scan in Progress	Indicates that a scan of your content is in progress.	3
Keylogger	Indicates that a key logger was detected.	7
Adware Detected	Indicates that Ad-Ware was detected.	4

**Table 93: Low-level categories and severity levels for the malware events category (continued)**

Low-level event category	Description	Severity level (0 - 10)
Quarantine Successful	Indicates that a quarantine action successfully completed.	3
Quarantine Failed	Indicates that a quarantine action failed.	8

## Suspicious Activity

The suspicious category contains events that are related to viruses, trojans, back door attacks, and other forms of hostile software.

The following table describes the low-level event categories and associated severity levels for the suspicious activity category.

**Table 94: Low-level categories and severity levels for the suspicious activity events category**

Low-level event category	Description	Severity level (0 - 10)
Unknown Suspicious Event	Indicates an unknown suspicious event.	3
Suspicious Pattern Detected	Indicates that a suspicious pattern was detected.	3
Content Modified By Firewall	Indicates that content was modified by the firewall.	3
Invalid Command or Data	Indicates an invalid command or data.	3
Suspicious Packet	Indicates a suspicious packet.	3
Suspicious Activity	Indicates suspicious activity.	3
Suspicious File Name	Indicates a suspicious file name.	3
Suspicious Port Activity	Indicates suspicious port activity.	3
Suspicious Routing	Indicates suspicious routing.	3
Potential Web Vulnerability	Indicates potential web vulnerability.	3
Unknown Evasion Event	Indicates an unknown evasion event.	5
IP Spoof	Indicates an IP spoof.	5
IP Fragmentation	Indicates IP fragmentation.	3
Overlapping IP Fragments	Indicates overlapping IP fragments.	5
IDS Evasion	Indicates an IDS evasion.	5
DNS Protocol Anomaly	Indicates a DNS protocol anomaly.	3
FTP Protocol Anomaly	Indicates an FTP protocol anomaly.	3
Mail Protocol Anomaly	Indicates a mail protocol anomaly.	3
Routing Protocol Anomaly	Indicates a routing protocol anomaly.	3
Web Protocol Anomaly	Indicates a web protocol anomaly.	3

**Table 94: Low-level categories and severity levels for the suspicious activity events category (continued)**

Low-level event category	Description	Severity level (0 - 10)
SQL Protocol Anomaly	Indicates an SQL protocol anomaly.	3
Executable Code Detected	Indicates that an executable code was detected.	5
Misc Suspicious Event	Indicates a miscellaneous suspicious event.	3
Information Leak	Indicates an information leak.	1
Potential Mail Vulnerability	Indicates a potential vulnerability in the mail server.	4
Potential Version Vulnerability	Indicates a potential vulnerability in the Extreme Networks Security Analytics version.	4
Potential FTP Vulnerability	Indicates a potential FTP vulnerability.	4
Potential SSH Vulnerability	Indicates a potential SSH vulnerability.	4
Potential DNS Vulnerability	Indicates a potential vulnerability in the DNS server.	4
Potential SMB Vulnerability	Indicates a potential SMB (Samba) vulnerability.	4
Potential Database Vulnerability	Indicates a potential vulnerability in the database.	4
IP Protocol Anomaly	Indicates a potential IP protocol anomaly	3
Suspicious IP Address	Indicates that a suspicious IP address was detected.	2
Invalid IP Protocol Usage	Indicates an invalid IP protocol.	2
Invalid Protocol	Indicates an invalid protocol.	4
Suspicious Window Events	Indicates a suspicious event with a screen on your desktop.	2
Suspicious ICMP Activity	Indicates suspicious ICMP activity.	2
Potential NFS Vulnerability	Indicates a potential network file system (NFS) vulnerability.	4
Potential NNTP Vulnerability	Indicates a potential Network News Transfer Protocol (NNTP) vulnerability.	4
Potential RPC Vulnerability	Indicates a potential RPC vulnerability.	4
Potential Telnet Vulnerability	Indicates a potential Telnet vulnerability on your system.	4
Potential SNMP Vulnerability	Indicates a potential SNMP vulnerability.	4
Illegal TCP Flag Combination	Indicates that an invalid TCP flag combination was detected.	5
Suspicious TCP Flag Combination	Indicates that a potentially invalid TCP flag combination was detected.	4
Illegal ICMP Protocol Usage	Indicates that an invalid use of the ICMP protocol was detected.	5
Suspicious ICMP Protocol Usage	Indicates that a potentially invalid use of the ICMP protocol was detected.	4
Illegal ICMP Type	Indicates that an invalid ICMP type was detected.	5
Illegal ICMP Code	Indicates that an invalid ICMP code was detected.	5



**Table 94: Low-level categories and severity levels for the suspicious activity events category (continued)**

Low-level event category	Description	Severity level (0 - 10)
Suspicious ICMP Type	Indicates that a potentially invalid ICMP type was detected.	4
Suspicious ICMP Code	Indicates that a potentially invalid ICMP code was detected.	4
TCP port 0	Indicates a TCP packet uses a reserved port (0) for source or destination.	4
UDP port 0	Indicates a UDP packet uses a reserved port (0) for source or destination.	4
Hostile IP	Indicates the use of a known hostile IP address.	4
Watch list IP	Indicates the use of an IP address from a watch list of IP addresses.	4
Known offender IP	Indicates the use of an IP address of a known offender.	4
RFC 1918 (private) IP	Indicates the use of an IP address from a private IP address range.	4
Potential VoIP Vulnerability	Indicates a potential VoIP vulnerability.	4
Blacklist Address	Indicates that an IP address is on the black list.	8
Watchlist Address	Indicates that the IP address is on the list of IP addresses being monitored.	7
Darknet Address	Indicates that the IP address is part of a darknet.	5
Botnet Address	Indicates that the address is part of a botnet.	7
Suspicious Address	Indicates that the IP address must be monitored.	5
Bad Content	Indicates that bad content was detected.	7
Invalid Cert	Indicates that an invalid certificate was detected.	7
User Activity	Indicates that user activity was detected.	7
Suspicious Protocol Usage	Indicates that suspicious protocol usage was detected.	5
Suspicious BGP Activity	Indicates that suspicious Border Gateway Protocol (BGP) usage was detected.	5
Route Poisoning	Indicates that route corruption was detected.	5
ARP Poisoning	Indicates that ARP-cache poisoning was detected.	5
Rogue Device Detected	Indicates that a rogue device was detected.	5

## System

The system category contains events that are related to system changes, software installation, or status messages.

The following table describes the low-level event categories and associated severity levels for the system category.

**Table 95: Low-level categories and severity levels for the system events category**

Low-level event category	Description	Severity level (0 - 10)
Unknown System Event	Indicates an unknown system event.	1
System Boot	Indicates a system restart.	1
System Configuration	Indicates a change in the system configuration.	1
System Halt	Indicates that the system was halted.	1
System Failure	Indicates a system failure.	6
System Status	Indicates any information event.	1
System Error	Indicates a system error.	3
Misc System Event	Indicates a miscellaneous system event.	1
Service Started	Indicates that system services started.	1
Service Stopped	Indicates that system services stopped.	1
Service Failure	Indicates a system failure.	6
Successful Registry Modification	Indicates that a modification to the registry was successful.	1
Successful Host-Policy Modification	Indicates that a modification to the host policy was successful.	1
Successful File Modification	Indicates that a modification to a file was successful.	1
Successful Stack Modification	Indicates that a modification to the stack was successful.	1
Successful Application Modification	Indicates that a modification to the application was successful.	1
Successful Configuration Modification	Indicates that a modification to the configuration was successful.	1
Successful Service Modification	Indicates that a modification to a service was successful.	1
Failed Registry Modification	Indicates that a modification to the registry failed.	1
Failed Host-Policy Modification	Indicates that a modification to the host policy failed.	1
Failed File Modification	Indicates that a modification to a file failed.	1
Failed Stack Modification	Indicates that a modification to the stack failed.	1
Failed Application Modification	Indicates that a modification to an application failed.	1
Failed Configuration Modification	Indicates that a modification to the configuration failed.	1
Failed Service Modification	Indicates that a modification to the service failed.	1
Registry Addition	Indicates that a new item was added to the registry.	1
Host-Policy Created	Indicates that a new entry was added to the registry.	1
File Created	Indicates that a new was created in the system.	1
Application Installed	Indicates that a new application was installed on the system.	1
Service Installed	Indicates that a new service was installed on the system.	1

**Table 95: Low-level categories and severity levels for the system events category (continued)**

Low-level event category	Description	Severity level (0 - 10)
Registry Deletion	Indicates that a registry entry was deleted.	1
Host-Policy Deleted	Indicates that a host policy entry was deleted.	1
File Deleted	Indicates that a file was deleted.	1
Application Uninstalled	Indicates that an application was uninstalled.	1
Service Uninstalled	Indicates that a service was uninstalled.	1
System Informational	Indicates system information.	3
System Action Allow	Indicates that an attempted action on the system was authorized.	3
System Action Deny	Indicates that an attempted action on the system was denied.	4
Cron	Indicates a crontab message.	1
Cron Status	Indicates a crontab status message.	1
Cron Failed	Indicates a crontab failure message.	4
Cron Successful	Indicates a crontab success message.	1
Daemon	Indicates a daemon message.	1
Daemon Status	Indicates a daemon status message.	1
Daemon Failed	Indicates a daemon failure message.	4
Daemon Successful	Indicates a daemon success message.	1
Kernel	Indicates a kernel message.	1
Kernel Status	Indicates a kernel status message.	1
Kernel Failed	Indicates a kernel failure message.	
Kernel Successful	Indicates a kernel successful message.	1
Authentication	Indicates an authentication message.	1
Information	Indicates an informational message.	2
Notice	Indicates a notice message.	3
Warning	Indicates a warning message.	5
Error	Indicates an error message.	7
Critical	Indicates a critical message.	9
Debug	Indicates a debug message.	1
Messages	Indicates a generic message.	1
Privilege Access	Indicates that privilege access was attempted.	3
Alert	Indicates an alert message.	9
Emergency	Indicates an emergency message.	9
SNMP Status	Indicates an SNMP status message.	1

**Table 95: Low-level categories and severity levels for the system events category (continued)**

Low-level event category	Description	Severity level (0 - 10)
FTP Status	Indicates an FTP status message.	1
NTP Status	Indicates an NTP status message.	1
Access Point Radio Failure	Indicates an access point radio failure.	3
Encryption Protocol Configuration Mismatch	Indicates an encryption protocol configuration mismatch.	3
Client Device or Authentication Server Misconfigured	Indicates that a client device or authentication server was not configured properly.	5
Hot Standby Enable Failed	Indicates a hot standby enable failure.	5
Hot Standby Disable Failed	Indicates a hot standby disable failure.	5
Hot Standby Enabled Successfully	Indicates that hot standby was enabled successfully.	1
Hot Standby Association Lost	Indicates that a hot standby association was lost.	5
MainMode Initiation Failure	Indicates MainMode initiation failure.	5
MainMode Initiation Succeeded	Indicates that the MainMode initiation was successful.	1
MainMode Status	Indicates a MainMode status message was reported.	1
QuickMode Initiation Failure	Indicates that the QuickMode initiation failed.	5
Quickmode Initiation Succeeded	Indicates that the QuickMode initiation was successful.	1
Quickmode Status	Indicates a QuickMode status message was reported.	1
Invalid License	Indicates an invalid license.	3
License Expired	Indicates an expired license.	3
New License Applied	Indicates a new license applied.	1
License Error	Indicates a license error.	5
License Status	Indicates a license status message.	1
Configuration Error	Indicates that a configuration error was detected.	5
Service Disruption	Indicates that a service disruption was detected.	5
License Exceeded	Indicates that the license capabilities were exceeded.	3
Performance Status	Indicates that the performance status was reported.	1
Performance Degradation	Indicates that the performance is being degraded.	4
Misconfiguration	Indicates that an incorrect configuration was detected.	5

## Policy

The policy category contains events that are related to administration of network policy and the monitoring network resources for policy violations.

The following table describes the low-level event categories and associated severity levels for the policy category.

**Table 96: Low-level categories and severity levels for the policy category**

Low-level event category	Description	Severity level (0 - 10)
Unknown Policy Violation	Indicates an unknown policy violation.	2
Web Policy Violation	Indicates a web policy violation.	2
Remote Access Policy Violation	Indicates a remote access policy violation.	2
IRC/IM Policy Violation	Indicates an instant messenger policy violation.	2
P2P Policy Violation	Indicates a Peer-to-Peer (P2P) policy violation.	2
IP Access Policy Violation	Indicates an IP access policy violation.	2
Application Policy Violation	Indicates an application policy violation.	2
Database Policy Violation	Indicates a database policy violation.	2
Network Threshold Policy Violation	Indicates a network threshold policy violation.	2
Porn Policy Violation	Indicates a porn policy violation.	2
Games Policy Violation	Indicates a games policy violation.	2
Misc Policy Violation	Indicates a miscellaneous policy violation.	2
Compliance Policy Violation	Indicates a compliance policy violation.	2
Mail Policy Violation	Indicates a mail policy violation.	2
IRC Policy Violation	Indicates an IRC policy violation.	2
IM Policy Violation	Indicates a policy violation that is related to instant message (IM) activities.	2
VoIP Policy Violation	Indicates a VoIP policy violation.	2
Succeeded	Indicates a policy successful message.	1
Failed	Indicates a policy failure message.	4

## Unknown

The Unknown category contains events that are not parsed and therefore cannot be categorized.

The following table describes the low-level event categories and associated severity levels for the Unknown category.

**Table 97: Low-level categories and severity levels for the Unknown category**

Low-level event category	Description	Severity level (0 - 10)
Unknown	Indicates an unknown event.	3
Unknown Short Event	Indicates an unknown Short event.	3
Unknown Dragon Event	Indicates an unknown Dragon event.	3

**Table 97: Low-level categories and severity levels for the Unknown category (continued)**

Low-level event category	Description	Severity level (0 - 10)
Unknown Pix Firewall Event	Indicates an unknown Cisco Private Internet Exchange (PIX) Firewall event.	3
Unknown Tipping Point Event	Indicates an unknown HP TippingPoint event.	3
Unknown Windows Auth Server Event	Indicates an unknown Windows™ Auth Server event.	3
Unknown Nortel Event	Indicates an unknown Nortel event.	3
Stored	Indicates an unknown stored event.	3
Behavioral	Indicates an unknown behavioral event.	3
Threshold	Indicates an unknown threshold event.	3
Anomaly	Indicates an unknown anomaly event.	3

## CRE

The custom rule event (CRE) category contains events that are generated from an event rule.

The following table describes the low-level event categories and associated severity levels for the CRE category.

**Table 98: Low-level categories and severity levels for the CRE category**

Low-level event category	Description	Severity level (0 - 10)
Unknown CRE Event	Indicates an unknown custom rules engine event.	5
Single Event Rule Match	Indicates a single event rule match.	5
Event Sequence Rule Match	Indicates an event sequence rule match.	5

## Potential Exploit

The potential exploit category contains events that are related to potential application exploits and buffer overflow attempts.

The following table describes the low-level event categories and associated severity levels for the potential exploit category.

**Table 99: Low-level categories and severity levels for the potential exploit category**

Low-level event category	Description	Severity level (0 - 10)
Unknown Potential Exploit Attack	Indicates that a potential exploitative attack was detected.	7
Potential Buffer Overflow	Indicates that a potential buffer overflow was detected.	7

**Table 99: Low-level categories and severity levels for the potential exploit category (continued)**

Low-level event category	Description	Severity level (0 - 10)
Potential DNS Exploit	Indicates that a potentially exploitative attack through the DNS server was detected.	7
Potential Telnet Exploit	Indicates that a potentially exploitative attack through Telnet was detected.	7
Potential Linux™ Exploit	Indicates that a potentially exploitative attack through Linux was™ detected.	7
Potential UNIX Exploit	Indicates that a potentially exploitative attack through UNIX was detected.	7
Potential Windows™ Exploit	Indicates that a potentially exploitative attack through Windows was™ detected.	7
Potential Mail Exploit	Indicates that a potentially exploitative attack through mail was detected.	7
Potential Infrastructure Exploit	Indicates that a potential exploitative attack on the system infrastructure was detected.	7
Potential Misc Exploit	Indicates that a potentially exploitative attack was detected.	7
Potential Web Exploit	Indicates that a potentially exploitative attack through the web was detected.	7
Potential Botnet Connection	Indicates a potentially exploitative attack that uses botnet was detected.	6
Potential Worm Activity	Indicates a potential attack that uses worm activity was detected.	6

## User Defined

The User Defined category contains events that are related to user-defined objects

The following table describes the low-level event categories and associated severity levels for the User Defined category.

**Table 100: Low-level categories and severity levels for the User Defined category**

Low-level event category	Description	Severity level (0 - 10)
Custom Sentry Low	Indicates a low severity custom anomaly event.	3
Custom Sentry Medium	Indicates a medium severity custom anomaly event.	5
Custom Sentry High	Indicates a high severity custom anomaly event.	7
Custom Sentry 1	Indicates a custom anomaly event with a severity level of 1.	1
Custom Sentry 2	Indicates a custom anomaly event with a severity level of 2.	2
Custom Sentry 3	Indicates a custom anomaly event with a severity level of 3.	3
Custom Sentry 4	Indicates a custom anomaly event with a severity level of 4.	4

**Table 100: Low-level categories and severity levels for the User Defined category (continued)**

Low-level event category	Description	Severity level (0 - 10)
Custom Sentry 5	Indicates a custom anomaly event with a severity level of 5.	5
Custom Sentry 6	Indicates a custom anomaly event with a severity level of 6.	6
Custom Sentry 7	Indicates a custom anomaly event with a severity level of 7.	7
Custom Sentry 8	Indicates a custom anomaly event with a severity level of 8.	8
Custom Sentry 9	Indicates a custom anomaly event with a severity level of 9.	9
Custom Policy Low	Indicates a custom policy event with a low severity level.	3
Custom Policy Medium	Indicates a custom policy event with a medium severity level.	5
Custom Policy High	Indicates a custom policy event with a high severity level.	7
Custom Policy 1	Indicates a custom policy event with a severity level of 1.	1
Custom Policy 2	Indicates a custom policy event with a severity level of 2.	2
Custom Policy 3	Indicates a custom policy event with a severity level of 3.	3
Custom Policy 4	Indicates a custom policy event with a severity level of 4.	4
Custom Policy 5	Indicates a custom policy event with a severity level of 5.	5
Custom Policy 6	Indicates a custom policy event with a severity level of 6.	6
Custom Policy 7	Indicates a custom policy event with a severity level of 7.	7
Custom Policy 8	Indicates a custom policy event with a severity level of 8.	8
Custom Policy 9	Indicates a custom policy event with a severity level of 9.	9
Custom User Low	Indicates a custom user event with a low severity level.	3
Custom User Medium	Indicates a custom user event with a medium severity level.	5
Custom User High	Indicates a custom user event with a high severity level.	7
Custom User 1	Indicates a custom user event with a severity level of 1.	1
Custom User 2	Indicates a custom user event with a severity level of 2.	2
Custom User 3	Indicates a custom user event with a severity level of 3.	3
Custom User 4	Indicates a custom user event with a severity level of 4.	4
Custom User 5	Indicates a custom user event with a severity level of 5.	5
Custom User 6	Indicates a custom user event with a severity level of 6.	6
Custom User 7	Indicates a custom user event with a severity level of 7.	7
Custom User 8	Indicates a custom user event with a severity level of 8.	8
Custom User 9	Indicates a custom user event with a severity level of 9.	9

## SIM Audit

The SIM Audit category contains events that are related to user interaction with the Extreme Security Console and administrative features.



The following table describes the low-level event categories and associated severity levels for the SIM Audit category.

**Table 101: Low-level categories and severity levels for the SIM Audit category**

Low-level event category	Description	Severity level (0 - 10)
SIM User Authentication	Indicates a user login or logout on the Console.	5
SIM Configuration Change	Indicates that a user changed the SIM configuration or deployment.	3
SIM User Action	Indicates that a user initiated a process, such as starting a backup or generating a report, in the SIM module.	3
Session Created	Indicates that a user session was created.	3
Session Destroyed	Indicates that a user session was destroyed.	3
Admin Session Created	Indicates that an admin session was created.	
Admin Session Destroyed	Indicates that an admin session was destroyed.	3
Session Authentication Invalid	Indicates an invalid session authentication.	5
Session Authentication Expired	Indicates that a session authentication expired.	3
Risk Manager Configuration	Indicates that a user changed the Extreme Networks Security Risk Manager configuration.	3

## VIS Host Discovery

When the VIS component discovers and stores new hosts, ports, or vulnerabilities that are detected on the network, the VIS component generates events. These events are sent to the Event Collector to be correlated with other security events.

The following table describes the low-level event categories and associated severity levels for the VIS host discovery category.

**Table 102: Low-level categories and severity levels for the VIS host discovery category**

Low-level event category	Description	Severity level (0 - 10)
New Host Discovered	Indicates that the VIS component detected a new host.	3
New Port Discovered	Indicates that the VIS component detected a new open port.	3
New Vuln Discovered	Indicates that the VIS component detected a new vulnerability.	3
New OS Discovered	Indicates that the VIS component detected a new operating system on a host.	3
Bulk Host Discovered	Indicates that the VIS component detected many new hosts in a short period.	3

## Application

The application category contains events that are related to application activity, such as email or FTP activity.

The following table describes the low-level event categories and associated severity levels for the application category.

**Table 103: Low-level categories and severity levels for the application category**

Low-level event category	Description	Severity level (0 - 10)
Mail Opened	Indicates that an email connection was established.	1
Mail Closed	Indicates that an email connection was closed.	1
Mail Reset	Indicates that an email connection was reset.	3
Mail Terminated	Indicates that an email connection was terminated.	4
Mail Denied	Indicates that an email connection was denied.	4
Mail in Progress	Indicates that an email connection is being attempted.	1
Mail Delayed	Indicates that an email connection was delayed.	4
Mail Queued	Indicates that an email connection was queued.	3
Mail Redirected	Indicates that an email connection was redirected.	1
FTP Opened	Indicates that an FTP connection was opened.	1
FTP Closed	Indicates that an FTP connection was closed.	1
FTP Reset	Indicates that an FTP connection was reset.	3
FTP Terminated	Indicates that an FTP connection was terminated.	4
FTP Denied	Indicates that an FTP connection was denied.	4
FTP In Progress	Indicates that an FTP connection is in progress.	1
FTP Redirected	Indicates that an FTP connection was redirected.	3
HTTP Opened	Indicates that an HTTP connection was established.	1
HTTP Closed	Indicates that an HTTP connection was closed.	1
HTTP Reset	Indicates that an HTTP connection was reset.	3
HTTP Terminated	Indicates that an HTTP connection was terminated.	4
HTTP Denied	Indicates that an HTTP connection was denied.	4
HTTP In Progress	Indicates that an HTTP connection is in progress.	1
HTTP Delayed	Indicates that an HTTP connection was delayed.	3
HTTP Queued	Indicates that an HTTP connection was queued.	1
HTTP Redirected	Indicates that an HTTP connection was redirected.	1
HTTP Proxy	Indicates that an HTTP connection is being proxied.	1
HTTPS Opened	Indicates that an HTTPS connection was established.	1
HTTPS Closed	Indicates that an HTTPS connection was closed.	1
HTTPS Reset	Indicates that an HTTPS connection was reset.	3

**Table 103: Low-level categories and severity levels for the application category (continued)**

Low-level event category	Description	Severity level (0 - 10)
HTTPS Terminated	Indicates that an HTTPS connection was terminated.	4
HTTPS Denied	Indicates that an HTTPS connection was denied.	4
HTTPS In Progress	Indicates that an HTTPS connection is in progress.	1
HTTPS Delayed	Indicates that an HTTPS connection was delayed.	3
HTTPS Queued	Indicates that an HTTPS connection was queued.	3
HTTPS Redirected	Indicates that an HTTPS connection was redirected.	3
HTTPS Proxy	Indicates that an HTTPS connection is proxied.	1
SSH Opened	Indicates that an SSH connection was established.	1
SSH Closed	Indicates that an SSH connection was closed.	1
SSH Reset	Indicates that an SSH connection was reset.	3
SSH Terminated	Indicates that an SSH connection was terminated.	4
SSH Denied	Indicates that an SSH session was denied.	4
SSH In Progress	Indicates that an SSH session is in progress.	1
RemoteAccess Opened	Indicates that a remote access connection was established.	1
RemoteAccess Closed	Indicates that a remote access connection was closed.	1
RemoteAccess Reset	Indicates that a remote access connection was reset.	3
RemoteAccess Terminated	Indicates that a remote access connection was terminated.	4
RemoteAccess Denied	Indicates that a remote access connection was denied.	4
RemoteAccess In Progress	Indicates that a remote access connection is in progress.	1
RemoteAccess Delayed	Indicates that a remote access connection was delayed.	3
RemoteAccess Redirected	Indicates that a remote access connection was redirected.	3
VPN Opened	Indicates that a VPN connection was opened.	1
VPN Closed	Indicates that a VPN connection was closed.	1
VPN Reset	Indicates that a VPN connection was reset.	3
VPN Terminated	Indicates that a VPN connection was terminated.	4
VPN Denied	Indicates that a VPN connection was denied.	4
VPN In Progress	Indicates that a VPN connection is in progress.	1
VPN Delayed	Indicates that a VPN connection was delayed.	3
VPN Queued	Indicates that a VPN connection was queued.	3
VPN Redirected	Indicates that a VPN connection was redirected.	3
RDP Opened	Indicates that an RDP connection was established.	1
RDP Closed	Indicates that an RDP connection was closed.	1
RDP Reset	Indicates that an RDP connection was reset.	3

**Table 103: Low-level categories and severity levels for the application category (continued)**

Low-level event category	Description	Severity level (0 - 10)
RDP Terminated	Indicates that an RDP connection was terminated.	4
RDP Denied	Indicates that an RDP connection was denied.	4
RDP In Progress	Indicates that an RDP connection is in progress.	1
RDP Redirected	Indicates that an RDP connection was redirected.	3
FileTransfer Opened	Indicates that a file transfer connection was established.	1
FileTransfer Closed	Indicates that a file transfer connection was closed.	1
FileTransfer Reset	Indicates that a file transfer connection was reset.	3
FileTransfer Terminated	Indicates that a file transfer connection was terminated.	4
FileTransfer Denied	Indicates that a file transfer connection was denied.	4
FileTransfer In Progress	Indicates that a file transfer connection is in progress.	1
FileTransfer Delayed	Indicates that a file transfer connection was delayed.	3
FileTransfer Queued	Indicates that a file transfer connection was queued.	3
FileTransfer Redirected	Indicates that a file transfer connection was redirected.	3
DNS Opened	Indicates that a DNS connection was established.	1
DNS Closed	Indicates that a DNS connection was closed.	1
DNS Reset	Indicates that a DNS connection was reset.	5
DNS Terminated	Indicates that a DNS connection was terminated.	5
DNS Denied	Indicates that a DNS connection was denied.	5
DNS In Progress	Indicates that a DNS connection is in progress.	1
DNS Delayed	Indicates that a DNS connection was delayed.	5
DNS Redirected	Indicates that a DNS connection was redirected.	4
Chat Opened	Indicates that a chat connection was opened.	1
Chat Closed	Indicates that a chat connection was closed.	1
Chat Reset	Indicates that a chat connection was reset.	3
Chat Terminated	Indicates that a chat connection was terminated.	3
Chat Denied	Indicates that a chat connection was denied.	3
Chat In Progress	Indicates that a chat connection is in progress.	1
Chat Redirected	Indicates that a chat connection was redirected.	1
Database Opened	Indicates that a database connection was established.	1
Database Closed	Indicates that a database connection was closed.	1
Database Reset	Indicates that a database connection was reset.	5
Database Terminated	Indicates that a database connection was terminated.	5
Database Denied	Indicates that a database connection was denied.	5

**Table 103: Low-level categories and severity levels for the application category (continued)**

Low-level event category	Description	Severity level (0 - 10)
Database In Progress	Indicates that a database connection is in progress.	1
Database Redirected	Indicates that a database connection was redirected.	3
SMTP Opened	Indicates that an SMTP connection was established.	1
SMTP Closed	Indicates that an SMTP connection was closed.	1
SMTP Reset	Indicates that an SMTP connection was reset.	3
SMTP Terminated	Indicates that an SMTP connection was terminated.	5
SMTP Denied	Indicates that an SMTP connection was denied.	5
SMTP In Progress	Indicates that an SMTP connection is in progress.	1
SMTP Delayed	Indicates that an SMTP connection was delayed.	3
SMTP Queued	Indicates that an SMTP connection was queued.	3
SMTP Redirected	Indicates that an SMTP connection was redirected.	3
Auth Opened	Indicates that an authorization server connection was established.	1
Auth Closed	Indicates that an authorization server connection was closed.	1
Auth Reset	Indicates that an authorization server connection was reset.	3
Auth Terminated	Indicates that an authorization server connection was terminated.	4
Auth Denied	Indicates that an authorization server connection was denied.	4
Auth In Progress	Indicates that an authorization server connection is in progress.	1
Auth Delayed	Indicates that an authorization server connection was delayed.	3
Auth Queued	Indicates that an authorization server connection was queued.	3
Auth Redirected	Indicates that an authorization server connection was redirected.	2
P2P Opened	Indicates that a Peer-to-Peer (P2P) connection was established.	1
P2P Closed	Indicates that a P2P connection was closed.	1
P2P Reset	Indicates that a P2P connection was reset.	4
P2P Terminated	Indicates that a P2P connection was terminated.	4
P2P Denied	Indicates that a P2P connection was denied.	3
P2P In Progress	Indicates that a P2P connection is in progress.	1
Web Opened	Indicates that a web connection was established.	1
Web Closed	Indicates that a web connection was closed.	1

**Table 103: Low-level categories and severity levels for the application category (continued)**

Low-level event category	Description	Severity level (0 - 10)
Web Reset	Indicates that a web connection was reset.	4
Web Terminated	Indicates that a web connection was terminated.	4
Web Denied	Indicates that a web connection was denied.	4
Web In Progress	Indicates that a web connection is in progress.	1
Web Delayed	Indicates that a web connection was delayed.	3
Web Queued	Indicates that a web connection was queued.	1
Web Redirected	Indicates that a web connection was redirected.	1
Web Proxy	Indicates that a web connection was proxied.	1
VoIP Opened	Indicates that a Voice Over IP (VoIP) connection was established.	1
VoIP Closed	Indicates that a VoIP connection was closed.	1
VoIP Reset	Indicates that a VoIP connection was reset.	3
VoIP Terminated	Indicates that a VoIP connection was terminated.	3
VoIP Denied	Indicates that a VoIP connection was denied.	3
VoIP In Progress	Indicates that a VoIP connection is in progress.	1
VoIP Delayed	Indicates that a VoIP connection was delayed.	3
VoIP Redirected	Indicates that a VoIP connection was redirected.	3
LDAP Session Started	Indicates an LDAP session started.	1
LDAP Session Ended	Indicates an LDAP session ended.	1
LDAP Session Denied	Indicates that an LDAP session was denied.	3
LDAP Session Status	Indicates that an LDAP session status message was reported.	1
LDAP Authentication Failed	Indicates that an LDAP authentication failed.	4
LDAP Authentication Succeeded	Indicates that an LDAP authentication was successful.	1
AAA Session Started	Indicates that an Authentication, Authorization, and Accounting (AAA) session started.	1
AAA Session Ended	Indicates that an AAA session ended.	1
AAA Session Denied	Indicates that an AAA session was denied.	3
AAA Session Status	Indicates that an AAA session status message was reported.	1
AAA Authentication Failed	Indicates that an AAA authentication failed.	4
AAA Authentication Succeeded	Indicates that an AAA authentication was successful.	1
IPSEC Authentication Failed	Indicates that an Internet Protocol Security (IPSEC) authentication failed.	4

**Table 103: Low-level categories and severity levels for the application category (continued)**

Low-level event category	Description	Severity level (0 - 10)
IPSEC Authentication Succeeded	Indicates that an IPSEC authentication was successful.	1
IPSEC Session Started	Indicates that an IPSEC session started.	1
IPSEC Session Ended	Indicates that an IPSEC session ended.	1
IPSEC Error	Indicates that an IPSEC error message was reported.	5
IPSEC Status	Indicates that an IPSEC session status message was reported.	1
IM Session Opened	Indicates that an Instant Messenger (IM) session was established.	1
IM Session Closed	Indicates that an IM session was closed.	1
IM Session Reset	Indicates that an IM session was reset.	3
IM Session Terminated	Indicates that an IM session was terminated.	3
IM Session Denied	Indicates that an IM session was denied.	3
IM Session In Progress	Indicates that an IM session is in progress.	1
IM Session Delayed	Indicates that an IM session was delayed	3
IM Session Redirected	Indicates that an IM session was redirected.	3
WHOIS Session Opened	Indicates that a WHOIS session was established.	1
WHOIS Session Closed	Indicates that a WHOIS session was closed.	1
WHOIS Session Reset	Indicates that a WHOIS session was reset.	3
WHOIS Session Terminated	Indicates that a WHOIS session was terminated.	3
WHOIS Session Denied	Indicates that a WHOIS session was denied.	3
WHOIS Session In Progress	Indicates that a WHOIS session is in progress.	1
WHOIS Session Redirected	Indicates that a WHOIS session was redirected.	3
Traceroute Session Opened	Indicates that a Traceroute session was established.	1
Traceroute Session Closed	Indicates that a Traceroute session was closed.	1
Traceroute Session Denied	Indicates that a Traceroute session was denied.	3
Traceroute Session In Progress	Indicates that a Traceroute session is in progress.	1
TN3270 Session Opened	TN3270 is a terminal emulation program, which is used to connect to a 3270 terminal. This category indicates that a TN3270 session was established.	1
TN3270 Session Closed	Indicates that a TN3270 session was closed.	1
TN3270 Session Reset	Indicates that a TN3270 session was reset.	3
TN3270 Session Terminated	Indicates that a TN3270 session was terminated.	3
TN3270 Session Denied	Indicates that a TN3270 session was denied.	3

**Table 103: Low-level categories and severity levels for the application category (continued)**

Low-level event category	Description	Severity level (0 - 10)
TN3270 Session In Progress	Indicates that a TN3270 session is in progress.	1
TFTP Session Opened	Indicates that a TFTP session was established.	1
TFTP Session Closed	Indicates that a TFTP session was closed.	1
TFTP Session Reset	Indicates that a TFTP session was reset.	3
TFTP Session Terminated	Indicates that a TFTP session was terminated.	3
TFTP Session Denied	Indicates that a TFTP session was denied.	3
TFTP Session In Progress	Indicates that a TFTP session is in progress.	1
Telnet Session Opened	Indicates that a Telnet session was established.	1
Telnet Session Closed	Indicates that a Telnet session was closed.	1
Telnet Session Reset	Indicates that a Telnet session was reset.	3
Telnet Session Terminated	Indicates that a Telnet session was terminated.	3
Telnet Session Denied	Indicates that a Telnet session was denied.	3
Telnet Session In Progress	Indicates that a Telnet session is in progress.	1
Syslog Session Opened	Indicates that a syslog session was established.	1
Syslog Session Closed	Indicates that a syslog session was closed.	1
Syslog Session Denied	Indicates that a syslog session was denied.	3
Syslog Session In Progress	Indicates that a syslog session is in progress.	1
SSL Session Opened	Indicates that a Secure Socket Layer (SSL) session was established.	1
SSL Session Closed	Indicates that an SSL session was closed.	1
SSL Session Reset	Indicates that an SSL session was reset.	3
SSL Session Terminated	Indicates that an SSL session was terminated.	3
SSL Session Denied	Indicates that an SSL session was denied.	3
SSL Session In Progress	Indicates that an SSL session is in progress.	1
SNMP Session Opened	Indicates that a Simple Network Management Protocol (SNMP) session was established.	1
SNMP Session Closed	Indicates that an SNMP session was closed.	1
SNMP Session Denied	Indicates that an SNMP session was denied.	3
SNMP Session In Progress	Indicates that an SNMP session is in progress.	1
SMB Session Opened	Indicates that a Server Message Block (SMB) session was established.	1
SMB Session Closed	Indicates that an SMB session was closed.	1
SMB Session Reset	Indicates that an SMB session was reset.	3
SMB Session Terminated	Indicates that an SMB session was terminated.	3
SMB Session Denied	Indicates that an SMB session was denied.	3



**Table 103: Low-level categories and severity levels for the application category (continued)**

Low-level event category	Description	Severity level (0 - 10)
SMB Session In Progress	Indicates that an SMB session is in progress.	1
Streaming Media Session Opened	Indicates that a Streaming Media session was established.	1
Streaming Media Session Closed	Indicates that a Streaming Media session was closed.	1
Streaming Media Session Reset	Indicates that a Streaming Media session was reset.	3
Streaming Media Session Terminated	Indicates that a Streaming Media session was terminated.	3
Streaming Media Session Denied	Indicates that a Streaming Media session was denied.	3
Streaming Media Session In Progress	Indicates that a Streaming Media session is in progress.	1
RUSERS Session Opened	Indicates that a (Remote Users) RUSERS session was established.	1
RUSERS Session Closed	Indicates that a RUSERS session was closed.	1
RUSERS Session Denied	Indicates that a RUSERS session was denied.	3
RUSERS Session In Progress	Indicates that a RUSERS session is in progress.	1
Rsh Session Opened	Indicates that a remote shell (rsh) session was established.	1
Rsh Session Closed	Indicates that an rsh session was closed.	1
Rsh Session Reset	Indicates that an rsh session was reset.	3
Rsh Session Terminated	Indicates that an rsh session was terminated.	3
Rsh Session Denied	Indicates that an rsh session was denied.	3
Rsh Session In Progress	Indicates that an rsh session is in progress.	1
RLOGIN Session Opened	Indicates that a Remote Login (RLOGIN) session was established.	1
RLOGIN Session Closed	Indicates that an RLOGIN session was closed.	1
RLOGIN Session Reset	Indicates that an RLOGIN session was reset.	3
RLOGIN Session Terminated	Indicates that an RLOGIN session was terminated.	3
RLOGIN Session Denied	Indicates that an RLOGIN session was denied.	3
RLOGIN Session In Progress	Indicates that an RLOGIN session is in progress.	1
REXEC Session Opened	Indicates that a (Remote Execution) REXEC session was established.	1
REXEC Session Closed	Indicates that an REXEC session was closed.	1
REXEC Session Reset	Indicates that an REXEC session was reset.	3

**Table 103: Low-level categories and severity levels for the application category (continued)**

Low-level event category	Description	Severity level (0 - 10)
REXEC Session Terminated	Indicates that an REXEC session was terminated.	3
REXEC Session Denied	Indicates that an REXEC session was denied.	3
REXEC Session In Progress	Indicates that an REXEC session is in progress.	1
RPC Session Opened	Indicates that a Remote Procedure Call (RPC) session was established.	1
RPC Session Closed	Indicates that an RPC session was closed.	1
RPC Session Reset	Indicates that an RPC session was reset.	3
RPC Session Terminated	Indicates that an RPC session was terminated.	3
RPC Session Denied	Indicates that an RPC session was denied.	3
RPC Session In Progress	Indicates that an RPC session is in progress.	1
NTP Session Opened	Indicates that a Network Time Protocol (NTP) session was established.	1
NTP Session Closed	Indicates that an NTP session was closed.	1
NTP Session Reset	Indicates that an NTP session was reset.	3
NTP Session Terminated	Indicates that an NTP session was terminated.	3
NTP Session Denied	Indicates that an NTP session was denied.	3
NTP Session In Progress	Indicates that an NTP session is in progress.	1
NNTP Session Opened	Indicates that a Network News Transfer Protocol (NNTP) session was established.	1
NNTP Session Closed	Indicates that an NNTP session was closed.	1
NNTP Session Reset	Indicates that an NNTP session was reset.	3
NNTP Session Terminated	Indicates that an NNTP session was terminated.	3
NNTP Session Denied	Indicates that an NNTP session was denied.	3
NNTP Session In Progress	Indicates that an NNTP session is in progress.	1
NFS Session Opened	Indicates that a Network File System (NFS) session was established.	1
NFS Session Closed	Indicates that an NFS session was closed.	1
NFS Session Reset	Indicates that an NFS session was reset.	3
NFS Session Terminated	Indicates that an NFS session was terminated.	3
NFS Session Denied	Indicates that an NFS session was denied.	3
NFS Session In Progress	Indicates that an NFS session is in progress.	1
NCP Session Opened	Indicates that a Network Control Program (NCP) session was established.	1
NCP Session Closed	Indicates that an NCP session was closed.	1
NCP Session Reset	Indicates that an NCP session was reset.	3

**Table 103: Low-level categories and severity levels for the application category (continued)**

Low-level event category	Description	Severity level (0 - 10)
NCP Session Terminated	Indicates that an NCP session was terminated.	3
NCP Session Denied	Indicates that an NCP session was denied.	3
NCP Session In Progress	Indicates that an NCP session is in progress.	1
NetBIOS Session Opened	Indicates that a NetBIOS session was established.	1
NetBIOS Session Closed	Indicates that a NetBIOS session was closed.	1
NetBIOS Session Reset	Indicates that a NetBIOS session was reset.	3
NetBIOS Session Terminated	Indicates that a NetBIOS session was terminated.	3
NetBIOS Session Denied	Indicates that a NetBIOS session was denied.	3
NetBIOS Session In Progress	Indicates that a NetBIOS session is in progress.	1
MODBUS Session Opened	Indicates that a MODBUS session was established.	1
MODBUS Session Closed	Indicates that a MODBUS session was closed.	1
MODBUS Session Reset	Indicates that a MODBUS session was reset.	3
MODBUS Session Terminated	Indicates that a MODBUS session was terminated.	3
MODBUS Session Denied	Indicates that a MODBUS session was denied.	3
MODBUS Session In Progress	Indicates that a MODBUS session is in progress.	1
LPD Session Opened	Indicates that a Line Printer Daemon (LPD) session was established.	1
LPD Session Closed	Indicates that an LPD session was closed.	1
LPD Session Reset	Indicates that an LPD session was reset.	3
LPD Session Terminated	Indicates that an LPD session was terminated.	3
LPD Session Denied	Indicates that an LPD session was denied.	3
LPD Session In Progress	Indicates that an LPD session is in progress.	1
Lotus Notes® Session Opened	Indicates that a Lotus Notes® session was established.	1
Lotus Notes® Session Closed	Indicates that a Lotus Notes® session was closed.	1
Lotus Notes® Session Reset	Indicates that a Lotus Notes® session was reset.	3
Lotus Notes® Session Terminated	Indicates that a Lotus Notes® session was terminated.	3
Lotus Notes® Session Denied	Indicates that a Lotus Notes® session was denied.	3
Lotus Notes® Session In Progress	Indicates that a Lotus Notes® session is in progress.	1

**Table 103: Low-level categories and severity levels for the application category (continued)**

Low-level event category	Description	Severity level (0 - 10)
Kerberos Session Opened	Indicates that a Kerberos session was established.	1
Kerberos Session Closed	Indicates that a Kerberos session was closed.	1
Kerberos Session Reset	Indicates that a Kerberos session was reset.	3
Kerberos Session Terminated	Indicates that a Kerberos session was terminated.	3
Kerberos Session Denied	Indicates that a Kerberos session was denied.	3
Kerberos Session In Progress	Indicates that a Kerberos session is in progress.	1
IRC Session Opened	Indicates that an Internet Relay Chat (IRC) session was established.	1
IRC Session Closed	Indicates that an IRC session was closed.	1
IRC Session Reset	Indicates that an IRC session was reset.	3
IRC Session Terminated	Indicates that an IRC session was terminated.	3
IRC Session Denied	Indicates that an IRC session was denied.	3
IRC Session In Progress	Indicates that an IRC session is in progress.	1
IEC 104 Session Opened	Indicates that an IEC 104 session was established.	1
IEC 104 Session Closed	Indicates that an IEC 104 session was closed.	1
IEC 104 Session Reset	Indicates that an IEC 104 session was reset.	3
IEC 104 Session Terminated	Indicates that an IEC 104 session was terminated.	3
IEC 104 Session Denied	Indicates that an IEC 104 session was denied.	3
IEC 104 Session In Progress	Indicates that an IEC 104 session is in progress.	1
Ident Session Opened	Indicates that a TCP Client Identity Protocol (Ident) session was established.	1
Ident Session Closed	Indicates that an Ident session was closed.	1
Ident Session Reset	Indicates that an Ident session was reset.	3
Ident Session Terminated	Indicates that an Ident session was terminated.	3
Ident Session Denied	Indicates that an Ident session was denied.	3
Ident Session In Progress	Indicates that an Ident session is in progress.	1
ICCP Session Opened	Indicates that an Inter-Control Center Communications Protocol (ICCP) session was established.	1
ICCP Session Closed	Indicates that an ICCP session was closed.	1
ICCP Session Reset	Indicates that an ICCP session was reset.	3
ICCP Session Terminated	Indicates that an ICCP session was terminated.	3
ICCP Session Denied	Indicates that an ICCP session was denied.	3
ICCP Session In Progress	Indicates that an ICCP session is in progress.	1

**Table 103: Low-level categories and severity levels for the application category (continued)**

Low-level event category	Description	Severity level (0 - 10)
GroupWiseSession Opened	Indicates that a GroupWisesession was established.	1
GroupWiseSession Closed	Indicates that a GroupWise session was closed.	1
GroupWiseSession Reset	Indicates that a GroupWisesession was reset.	3
GroupWiseSession Terminated	Indicates that a GroupWisesession was terminated.	3
GroupWiseSession Denied	Indicates that a GroupWise session was denied.	3
GroupWiseSession In Progress	Indicates that a GroupWise session is in progress.	1
Gopher Session Opened	Indicates that a Gopher session was established.	1
Gopher Session Closed	Indicates that a Gopher session was closed.	1
Gopher Session Reset	Indicates that a Gopher session was reset.	3
Gopher Session Terminated	Indicates that a Gopher session was terminated.	3
Gopher Session Denied	Indicates that a Gopher session was denied.	3
Gopher Session In Progress	Indicates that a Gopher session is in progress.	1
GIOP Session Opened	Indicates that a General Inter-ORB Protocol (GIOP) session was established.	1
GIOP Session Closed	Indicates that a GIOP session was closed.	1
GIOP Session Reset	Indicates that a GIOP session was reset.	3
GIOP Session Terminated	Indicates that a GIOP session was terminated.	3
GIOP Session Denied	Indicates that a GIOP session was denied.	3
GIOP Session In Progress	Indicates that a GIOP session is in progress.	1
Finger Session Opened	Indicates that a Finger session was established.	1
Finger Session Closed	Indicates that a Finger session was closed.	1
Finger Session Reset	Indicates that a Finger session was reset.	3
Finger Session Terminated	Indicates that a Finger session was terminated.	3
Finger Session Denied	Indicates that a Finger session was denied.	3
Finger Session In Progress	Indicates that a Finger session is in progress.	1
Echo Session Opened	Indicates that an Echo session was established.	1
Echo Session Closed	Indicates that an Echo session was closed.	1
Echo Session Denied	Indicates that an Echo session was denied.	3
Echo Session In Progress	Indicates that an Echo session is in progress.	1
Remote .NET Session Opened	Indicates that a Remote .NET session was established.	1
Remote .NET Session Closed	Indicates that a Remote .NET session was closed.	1

**Table 103: Low-level categories and severity levels for the application category (continued)**

Low-level event category	Description	Severity level (0 - 10)
Remote .NET Session Reset	Indicates that a Remote .NET session was reset.	3
Remote .NET Session Terminated	Indicates that a Remote .NET session was terminated.	3
Remote .NET Session Denied	Indicates that a Remote .NET session was denied.	3
Remote .NET Session In Progress	Indicates that a Remote .NET session is in progress.	1
DNP3 Session Opened	Indicates that a Distributed Network Proctologic (DNP3) session was established.	1
DNP3 Session Closed	Indicates that a DNP3 session was closed.	1
DNP3 Session Reset	Indicates that a DNP3 session was reset.	3
DNP3 Session Terminated	Indicates that a DNP3 session was terminated.	3
DNP3 Session Denied	Indicates that a DNP3 session was denied.	3
DNP3 Session In Progress	Indicates that a DNP3 session is in progress.	1
Discard Session Opened	Indicates that a Discard session was established.	1
Discard Session Closed	Indicates that a Discard session was closed.	1
Discard Session Reset	Indicates that a Discard session was reset.	3
Discard Session Terminated	Indicates that a Discard session was terminated.	3
Discard Session Denied	Indicates that a Discard session was denied.	3
Discard Session In Progress	Indicates that a Discard session is in progress.	1
DHCP Session Opened	Indicates that a Dynamic Host Configuration Protocol (DHCP) session was established.	1
DHCP Session Closed	Indicates that a DHCP session was closed.	1
DHCP Session Denied	Indicates that a DHCP session was denied.	3
DHCP Session In Progress	Indicates that a DHCP session is in progress.	1
DHCP Success	Indicates that a DHCP lease was successfully obtained	1
DHCP Failure	Indicates that a DHCP lease cannot be obtained.	3
CVS Session Opened	Indicates that a Concurrent Versions System (CVS) session was established.	1
CVS Session Closed	Indicates that a CVS session was closed.	1
CVS Session Reset	Indicates that a CVS session was reset.	3
CVS Session Terminated	Indicates that a CVS session was terminated.	3
CVS Session Denied	Indicates that a CVS session was denied.	3
CVS Session In Progress	Indicates that a CVS session is in progress.	1
CUPS Session Opened	Indicates that a Common UNIX™ Printing System (CUPS) session was established.	1

**Table 103: Low-level categories and severity levels for the application category (continued)**

Low-level event category	Description	Severity level (0 - 10)
CUPS Session Closed	Indicates that a CUPS session was closed.	1
CUPS Session Reset	Indicates that a CUPS session was reset.	3
CUPS Session Terminated	Indicates that a CUPS session was terminated.	3
CUPS Session Denied	Indicates that a CUPS session was denied.	3
CUPS Session In Progress	Indicates that a CUPS session is in progress.	1
Chargen Session Started	Indicates that a Character Generator (Chargen) session was started.	1
Chargen Session Closed	Indicates that a Chargen session was closed.	1
Chargen Session Reset	Indicates that a Chargen session was reset.	3
Chargen Session Terminated	Indicates that a Chargen session was terminated.	3
Chargen Session Denied	Indicates that a Chargen session was denied.	3
Chargen Session In Progress	Indicates that a Chargen session is in progress.	1
Misc VPN	Indicates that a miscellaneous VPN session was detected	1
DAP Session Started	Indicates that a DAP session was established.	1
DAP Session Ended	Indicates that a DAP session ended.	1
DAP Session Denied	Indicates that a DAP session was denied.	3
DAP Session Status	Indicates that a DAP session status request was made.	1
DAP Session in Progress	Indicates that a DAP session is in progress.	1
DAP Authentication Failed	Indicates that a DAP authentication failed.	4
DAP Authentication Succeeded	Indicates that DAP authentication succeeded.	1
TOR Session Started	Indicates that a TOR session was established.	1
TOR Session Closed	Indicates that a TOR session was closed.	1
TOR Session Reset	Indicates that a TOR session was reset.	3
TOR Session Terminated	Indicates that a TOR session was terminated.	3
TOR Session Denied	Indicates that a TOR session was denied.	3
TOR Session In Progress	Indicates that a TOR session is in progress.	1
Game Session Started	Indicates that a game session was started.	1
Game Session Closed	Indicates that a game session was closed.	1
Game Session Reset	Indicates that a game session was reset.	3
Game Session Terminated	Indicates that a game session was terminated.	3
Game Session Denied	Indicates that a game session was denied.	3
Game Session In Progress	Indicates that a game session is in progress.	1

**Table 103: Low-level categories and severity levels for the application category (continued)**

Low-level event category	Description	Severity level (0 - 10)
Admin Login Attempt	Indicates that an attempt to log in as an administrative user was detected.	2
User Login Attempt	Indicates that an attempt to log in as a non-administrative user was detected.	2
Client Server	Indicates client/server activity.	1
Content Delivery	Indicates content delivery activity.	1
Data Transfer	Indicates a data transfer.	3
Data Warehousing	Indicates data warehousing activity.	3
Directory Services	Indicates directory service activity.	2
File Print	Indicates file print activity.	1
File Transfer	Indicates file transfer.	2
Games	Indicates game activity.	4
Healthcare	Indicates healthcare activity.	1
Inner System	Indicates inner system activity.	1
Internet Protocol	Indicates Internet Protocol activity.	1
Legacy	Indicates legacy activity.	1
Mail	Indicates mail activity.	1
Misc	Indicates miscellaneous activity.	2
Multimedia	Indicates multimedia activity.	2
Network Management	Indicates network management activity.	
P2P	Indicates Peer-to-Peer (P2P) activity.	4
Remote Access	Indicates Remote Access activity.	3
Routing Protocols	Indicates routing protocol activity.	1
Security Protocols	Indicates security protocol activity.	2
Streaming	Indicates streaming activity.	2
Uncommon Protocol	Indicates uncommon protocol activity.	3
VoIP	Indicates VoIP activity.	1
Web	Indicates web activity.	1
ICMP	Indicates ICMP activity	1

## Audit

The audit category contains events that are related to audit activity, such as email or FTP activity.

The following table describes the low-level event categories and associated severity levels for the audit category.



**Table 104: Low-level categories and severity levels for the audit category**

Low-level event category	Description	Severity level (0 - 10)
General Audit Event	Indicates that a general audit event was started.	1
Built-in Execution	Indicates that a built-in audit task was run.	1
Bulk Copy	Indicates that a bulk copy of data was detected.	1
Data Dump	Indicates that a data dump was detected.	1
Data Import	Indicates that a data import was detected.	1
Data Selection	Indicates that a data selection process was detected.	1
Data Truncation	Indicates that the data truncation process was detected.	1
Data Update	Indicates that the data update process was detected.	1
Procedure/Trigger Execution	Indicates that the database procedure or trigger execution was detected.	1
Schema Change	Indicates that the schema for a procedure or trigger execution was altered.	1

## Risk

The risk category contains events that are related to Extreme Networks Security Risk Manager.

The following table describes the low-level event categories and associated severity levels for the risk category.

**Table 105: Low-level categories and severity levels for the risk category**

Low-level event category	Description	Severity level (0 - 10)
Policy Exposure	Indicates that a policy exposure was detected.	5
Compliance Violation	Indicates that a compliance violation was detected.	5
Exposed Vulnerability	Indicates that the network or device has an exposed vulnerability.	9
Remote Access Vulnerability	Indicates that the network or device has a remote access vulnerability.	9
Local Access Vulnerability	Indicates that the network or device has local access vulnerability.	7
Open Wireless Access	Indicates that the network or device has open wireless access.	5
Weak Encryption	Indicates that the host or device has weak encryption.	5
Un-Encrypted Data Transfer	Indicates that a host or device is transmitting data that is not encrypted.	3
Un-Encrypted Data Store	Indicates that the data store is not encrypted.	3
Mis-Configured Rule	Indicates that a rule is not configured properly.	3

**Table 105: Low-level categories and severity levels for the risk category (continued)**

Low-level event category	Description	Severity level (0 - 10)
Mis-Configured Device	Indicates that a device on the network is not configured properly.	3
Mis-Configured Host	Indicates that a network host is not configured properly.	3
Data Loss Possible	Indicates that the possibility of data loss was detected.	5
Weak Authentication	Indicates that a host or device is susceptible to fraud.	5
No Password	Indicates that no password exists.	7
Fraud	Indicates that a host or device is susceptible to fraud.	7
Possible DoS Target	Indicates a host or device is a possible DoS target.	3
Possible DoS Weakness	Indicates a host or device has a possible DoS weakness.	3
Loss of Confidentiality	Indicates that a loss of confidentiality was detected.	5
Policy Monitor Risk Score Accumulation	Indicates that a policy monitor risk score accumulation was detected.	1

## Risk Manager Audit

The risk category contains events that are related to Extreme Networks Security Risk Manager audit events.

The following table describes the low-level event categories and associated severity levels for the Risk Manager audit category.

**Table 106: Low-level categories and severity levels for the Risk Manager audit category**

Low-level event category	Description	Severity level (0 - 10)
Policy Monitor	Indicates that a policy monitor was modified.	3
Topology	Indicates that a topology was modified.	3
Simulations	Indicates that a simulation was modified.	3
Administration	Indicates that administrative changes were made.	3

## Control

The control category contains events that are related to your hardware system.

The following table describes the low-level event categories and associated severity levels for the control category.

**Table 107: Low-level categories and severity levels for the control category**

Low-level event category	Description	Severity level (0 - 10)
Device Read	Indicates that a device was read.	1
Device Communication	Indicates communication with a device.	1
Device Audit	Indicates that a device audit occurred.	1
Device Event	Indicates that a device event occurred.	1
Device Ping	Indicates that a ping action to a device occurred.	1
Device Configuration	Indicates that a device was configured.	1
Device Route	Indicates that a device route action occurred.	1
Device Import	Indicates that a device import occurred.	1
Device Information	Indicates that a device information action occurred.	1
Device Warning	Indicates that a warning was generated on a device.	1
Device Error	Indicates that an error was generated on a device.	1
Relay Event	Indicates a relay event.	1
NIC Event	Indicates a Network Interface Card (NIC) event.	1
UIQ Event	Indicates an event on a mobile device.	1
IMU Event	Indicates an event on an Integrated Management Unit (IMU).	1
Billing Event	Indicates a billing event.	1
DBMS Event	Indicates an event on the Database Management System (DBMS).	1
Import Event	Indicates that an import occurred.	1
Location Import	Indicates that a location import occurred.	1
Route Import	Indicates that a route import occurred.	1
Export Event	Indicates that an export occurred.	1
Remote Signalling	Indicates remote signaling.	1
Gateway Status	Indicates gateway status.	1
Job Event	Indicates that a job occurred.	1
Security Event	Indicates that a security event occurred.	1
Device Tamper Detection	Indicates that the system detected a tamper action.	1
Time Event	Indicates that a time event occurred.	1
Suspicious Behavior	Indicates that suspicious behavior occurred.	1
Power Outage	Indicates that a power outage occurred.	1
Power Restoration	Indicates that power was restored.	1
Heartbeat	Indicates that a heartbeat ping occurred.	1
Remote Connection Event	Indicates a remote connection to the system.	1

## Asset Profiler

The asset profiler category contains events that are related to asset profiles.

The following table describes the low-level event categories and associated severity levels for the asset profiler category.

**Table 108: Low-level categories and severity levels for the asset profiler category**

Low-level event category	Description	Severity level (0 - 10)
Asset Created	Indicates that an asset was created.	1
Asset Updated	Indicates that an asset was updated.	1
Asset Observed	Indicates that an asset was observed.	1
Asset Moved	Indicates that an asset was moved.	1
Asset Deleted	Indicates that an asset was deleted.	1
Asset Hostname Cleaned	Indicates that a host name was cleaned.	1
Asset Hostname Created	Indicates that a host name was created.	1
Asset Hostname Updated	Indicates that a host name was updated.	1
Asset Hostname Observed	Indicates that a host name was observed.	1
Asset Hostname Moved	Indicates that a host name was moved.	1
Asset Hostname Deleted	Indicates that a host name was deleted.	1
Asset Port Cleaned	Indicates that a port was cleaned.	1
Asset Port Created	Indicates that a port was created.	1
Asset Port Updated	Indicates that a port was updated.	1
Asset Port Observed	Indicates that a port was observed.	1
Asset Port Moved	Indicates that a port was moved.	1
Asset Port Deleted	Indicates that a port was deleted.	1
Asset Vuln Instance Cleaned	Indicates that a vulnerability instance was cleaned.	1
Asset Vuln Instance Created	Indicates that a vulnerability instance was created.	1
Asset Vuln Instance Updated	Indicates that a vulnerability instance was updated.	1
Asset Vuln Instance Observed	Indicates that a vulnerability instance was observed.	1
Asset Vuln Instance Moved	Indicates that a vulnerability instance was moved.	1
Asset Vuln Instance Deleted	Indicates that a vulnerability instance was deleted.	1
Asset OS Cleaned	Indicates that an operating system was cleaned.	1
Asset OS Created	Indicates that an operating system was created.	1
Asset OS Updated	Indicates that an operating system was updated.	1
Asset OS Observed	Indicates that an operating system was observed.	1
Asset OS Moved	Indicates that an operating system was moved.	1
Asset OS Deleted	Indicates that an operating system was deleted.	1

**Table 108: Low-level categories and severity levels for the asset profiler category (continued)**

Low-level event category	Description	Severity level (0 - 10)
Asset Property Cleaned	Indicates that a property was cleaned.	1
Asset Property Created	Indicates that a property was created.	1
Asset Property Updated	Indicates that a property was updated.	1
Asset Property Observed	Indicates that a property was observed.	1
Asset Property Moved	Indicates that a property was moved.	1
Asset Property Deleted	Indicates that a property was moved.	1
Asset IP Address Cleaned	Indicates that an IP address was cleaned.	1
Asset IP Address Created	Indicates that an IP address was created.	1
Asset IP Address Updated	Indicates that an IP address was updated.	1
Asset IP Address Observed	Indicates that an IP address was observed.	1
Asset IP Address Moved	Indicates that an IP address was moved.	1
Asset IP Address Deleted	Indicates that an IP address was deleted.	1
Asset Interface Cleaned	Indicates that an interface was cleaned.	1
Asset Interface Created	Indicates that an interface was created.	1
Asset Interface Updated	Indicates that an interface was updated.	1
Asset Interface Observed	Indicates that an interface was observed.	1
Asset Interface Moved	Indicates that an interface was moved.	1
Asset Interface Merged	Indicates that an interface was merged.	1
Asset Interface Deleted	Indicates that an interface was deleted.	1
Asset User Cleaned	Indicates that a user was cleaned.	1
Asset User Observed	Indicates that a user was observed.	1
Asset User Moved	Indicates that a user was moved.	1
Asset User Deleted	Indicates that a user was deleted.	1
Asset Scanned Policy Cleaned	Indicates that a scanned policy was cleaned.	1
Asset Scanned Policy Observed	Indicates that a scanned policy was observed.	1
Asset Scanned Policy Moved	Indicates that a scanned policy was moved.	1
Asset Scanned Policy Deleted	Indicates that a scanned policy was deleted.	1
Asset Windows™ Application Cleaned	Indicates that a Windows™ application was cleaned.	1
Asset Windows™ Application Observed	Indicates that a Windows™ application was observed.	1
Asset Windows™ Application Moved	Indicates that a Windows™ application was moved.	1
Asset Windows™ Application Deleted	Indicates that a Windows™ application was deleted.	1
Asset Scanned Service Cleaned	Indicates that a scanned service was cleaned.	1
Asset Scanned Service Observed	Indicates that a scanned service was observed.	1

**Table 108: Low-level categories and severity levels for the asset profiler category (continued)**

Low-level event category	Description	Severity level (0 - 10)
Asset Scanned Service Moved	Indicates that a scanned service was moved.	1
Asset Scanned Service Deleted	Indicates that a scanned service was deleted.	1
Asset Windows™ Patch Cleaned	Indicates that a Windows™ patch was cleaned.	1
Asset Windows™ Patch Observed	Indicates that a Windows™ patch was observed.	1
Asset Windows™ Patch Moved	Indicates that a Windows™ patch was moved.	1
Asset Windows™ Patch Deleted	Indicates that a Windows™ patch was deleted.	1
Asset UNIX™ Patch Cleaned	Indicates that a UNIX™ patch was cleaned.	1
Asset UNIX™ Patch Observed	Indicates that a UNIX™ patch was observed.	1
Asset UNIX™ Patch Moved	Indicates that a UNIX™ patch was moved.	1
Asset UNIX™ Patch Deleted	Indicates that a UNIX™ patch was deleted.	1
Asset Patch Scan Cleaned	Indicates that a patch scan was cleaned.	1
Asset Patch Scan Created	Indicates that a patch scan was created.	1
Asset Patch Scan Moved	Indicates that a patch scan was moved.	1
Asset Patch Scan Deleted	Indicates that a patch scan was deleted.	1
Asset Port Scan Cleaned	Indicates that a port scan was cleaned.	1
Asset Port Scan Created	Indicates that a port scan was cleaned.	1
Asset Port Scan Moved	Indicates that a patch scan was moved.	1
Asset Port Scan Deleted	Indicates that a patch scan was deleted.	1
Asset Client Application Cleaned	Indicates that a client application was cleaned.	1
Asset Client Application Observed	Indicates that a client application was observed.	1
Asset Client Application Moved	Indicates that a client application was moved.	1
Asset Client Application Deleted	Indicates that a client application was deleted.	1
Asset Patch Scan Observed	Indicates that a patch scan was observed.	1
Asset Port Scan Observed	Indicates that a port scan was observed.	1

# 20 Ports used by Extreme Security

## Searching for ports in use by Extreme Security Console Viewing IMQ port associations

Review the common ports that are used by Extreme Networks Security Analytics, services, and components.

For example, you can determine the ports that must be opened for the Extreme Security Console to communicate with remote Event Processors.

### Ports and iptables

The listen ports for Extreme Security are valid only when iptables is enabled on your Extreme Security system.

### SSH communication on port 22

All the ports that are described in following table can be tunneled, by encryption, through port 22 over SSH. Managed hosts that use encryption can establish multiple bidirectional SSH sessions to communicate securely. These SSH sessions are initiated from the managed host to provide data to the host that needs the data in the deployment. For example, Event Processor appliances can initiate multiple SSH sessions to the Extreme Security Console for secure communication. This communication can include tunneled ports over SSH, such as HTTPS data for port 443 and Ariel query data for port 32006.

### QRadar ports

Unless otherwise noted, information about the assigned port number, descriptions, protocols, and the signaling direction for the port applies to all Extreme Networks Security Analytics products. References to flows do not apply to Extreme Networks Security Log Manager.

The following table lists the ports, protocols, communication direction, description, and the reason that the port is used.

**Table 109: Listening ports that are used by QRadar, services, and components**

Port	Description	Protocol	Direction	Requirement
22	SSH	TCP	Bidirectional from the Extreme Security Console to all other components.	Remote management access Adding a remote system as a managed host Log source protocols to retrieve files from external devices, for example the log file protocol Users who use the command-line interface to communicate from desktops to the Console High-availability (HA)
25	SMTP	TCP	From all managed hosts to the SMTP gateway	Emails from Extreme Security to an SMTP gateway Delivery of error and warning email messages to an administrative email contact
37	rdate (time)	UDP/TCP	All systems to the Extreme Security Console Extreme Security Console to the NTP or rdate server	Time synchronization between the Extreme Security Console and managed hosts
111	Port mapper	TCP/UDP	Managed hosts that communicate to the Extreme Security Console Users that connect to the Extreme Security Console	Remote Procedure Calls (RPC) for required services, such as Network File System (NFS)



**Table 109: Listening ports that are used by QRadar, services, and components (continued)**

Port	Description	Protocol	Direction	Requirement
135 and dynamically allocated ports above 1024 for RPC calls.	DCOM	TCP	<p>WinCollect agents and Windows operating systems that are remotely polled for events.</p> <p>Bidirectional traffic between Extreme Security Console components that use the Microsoft Security Event Log Protocol and Windows operating systems that are remotely polled for events or bidirectional traffic between or Extreme Security Event Collectors that use the Microsoft Security Event Log Protocol and Windows operating systems that are remotely polled for events.</p> <p>Bidirectional traffic between Adaptive Log Exporter agents and Windows operating systems that are remotely polled for events.</p>	<p>This traffic is generated by WinCollect, Microsoft Security Event Log Protocol, or Adaptive Log Exporter.</p> <hr/> <p><b>Note</b> DCOM typically allocates a random port range for communication. You can configure Microsoft Windows products to use a specific port. For more information, see your Microsoft Windows documentation.</p>
137	Windows NetBIOS name service	UDP	<p>Bidirectional traffic between WinCollect agents and Windows operating systems that are remotely polled for events</p> <p>Bidirectional traffic between Extreme Security Console components or Extreme Security Event Collectors that use the Microsoft Security Event Log Protocol and Windows operating systems that are remotely polled for events.</p> <p>Bidirectional traffic between Adaptive Log Exporter agents and Windows operating systems that are remotely polled for events</p>	<p>This traffic is generated by WinCollect, Microsoft Security Event Log Protocol, or Adaptive Log Exporter.</p>

**Table 109: Listening ports that are used by QRadar, services, and components (continued)**

Port	Description	Protocol	Direction	Requirement
138	Windows NetBIOS datagram service	UDP	<p>Bidirectional traffic between WinCollect agents and Windows operating systems that are remotely polled for events</p> <p>Bidirectional traffic between Extreme Security Console components or Extreme Security Event Collectors that use the Microsoft Security Event Log Protocol and Windows operating systems that are remotely polled for events.</p> <p>Bidirectional traffic between Adaptive Log Exporter agents and Windows operating systems that are remotely polled for events</p>	This traffic is generated by WinCollect, Microsoft Security Event Log Protocol, or Adaptive Log Exporter.
139	Windows NetBIOS session service	TCP	<p>Bidirectional traffic between WinCollect agents and Windows operating systems that are remotely polled for events</p> <p>Bidirectional traffic between Extreme Security Console components or Extreme Security Event Collectors that use the Microsoft Security Event Log Protocol and Windows operating systems that are remotely polled for events.</p> <p>Bidirectional traffic between Adaptive Log Exporter agents and Windows operating systems that are remotely polled for events</p>	This traffic is generated by WinCollect, Microsoft Security Event Log Protocol, or Adaptive Log Exporter.
199	NetSNMP	TCP	<p>Extreme Security managed hosts that connect to the Extreme Security Console</p> <p>External log sources to Extreme Security Extreme Security Event Collectors</p>	TCP port for the NetSNMP daemon that listens for communications (v1, v2c, and v3) from external log sources
427	Service Location Protocol (SLP)	UDP/TCP		The Integrated Management Module uses the port to find services on a LAN.
443	Apache/HTTPS	TCP	Bidirectional traffic for secure communications from all products to the Extreme Security Console	<p>Configuration downloads to managed hosts from the Extreme Security Console</p> <p>Extreme Security managed hosts that connect to the Extreme Security Console Users to have log in access to Extreme Security</p> <p>Extreme Security Console that manage and provide configuration updates for WinCollect agents</p>

**Table 109: Listening ports that are used by QRadar, services, and components (continued)**

Port	Description	Protocol	Direction	Requirement
445	Microsoft Directory Service	TCP	<p>Bidirectional traffic between WinCollect agents and Windows operating systems that are remotely polled for events</p> <p>Bidirectional traffic between Extreme Security Console components or Extreme Security Event Collectors that use the Microsoft Security Event Log Protocol and Windows operating systems that are remotely polled for events</p> <p>Bidirectional traffic between Adaptive Log Exporter agents and Windows operating systems that are remotely polled for events</p>	This traffic is generated by WinCollect, Microsoft Security Event Log Protocol, or Adaptive Log Exporter.
514	Syslog	UDP/TCP	<p>External network appliances that provide TCP syslog events use bidirectional traffic.</p> <p>External network appliances that provide UDP syslog events use unidirectional traffic.</p>	External log sources to send event data to Extreme Security components Syslog traffic includes WinCollect agents and Adaptive Log Exporter agents capable of sending either UDP or TCP events to Extreme Security
762	Network File System (NFS) mount daemon (mountd)	TCP/UDP	Connections between the Extreme Security Console and NFS server	The Network File System (NFS) mount daemon, which processes requests to mount a file system at a specified location
1514	Syslog-ng	TCP/UDP	Connection between the local Event Collector component and local Event Processor component to the syslog-ng daemon for logging	Internal logging port for syslog-ng
2049	NFS	TCP	Connections between the Extreme Security Console and NFS server	The Network File System (NFS) protocol to share files or data between components
2055	NetFlow data	UDP	From the management interface on the flow source (typically a router) to the QFlow Collector.	NetFlow datagram from components, such as routers
3389	Remote Desktop Protocol (RDP) and Ethernet over USB is enabled	TCP/UDP		If the Windows operating system is configured to support RDP and Ethernet over USB, a user can initiate a session to the server over the management network. This means the default port for RDP, 3389 must be open.


**Table 109: Listening ports that are used by QRadar, services, and components (continued)**

Port	Description	Protocol	Direction	Requirement
3900	Integrated Management Module remote presence port	TCP/UDP		Use this port to interact with the Extreme Security console through the Integrated Management Module.
4333	Redirect port	TCP		This port is assigned as a redirect port for Address Resolution Protocol (ARP) requests in Extreme Security offense resolution
5432	Postgres	TCP	Communication for the managed host that is used to access the local database instance	Required for provisioning managed hosts from the <b>Admin</b> tab
6543	High-availability heartbeat	TCP/UDP	Bidirectional between the secondary host and primary host in an HA cluster	Heartbeat ping from a secondary host to a primary host in an HA cluster to detect hardware or network failure
7676, 7677, and four randomly bound ports above 32000.	Messaging connections (IMQ)	TCP	Message queue communications between components on a managed host.	Message queue broker for communications between components on a managed host Ports 7676 and 7677 are static TCP ports and four extra connections are created on random ports.
7777 - 7782, 7790, 7791	JMX server ports	TCP	Internal communications, these ports are not available externally	JMX server (Mbean) monitoring for ECS, host context, Tomcat, VIS, reporting, ariel, and accumulator services  <div><b>Note</b> These ports are used by Extreme Security support.</div>
7789	HA Distributed Replicated Block Device (DRBD)	TCP/UDP	Bidirectional between the secondary host and primary host in an HA cluster	Distributed Replicated Block Device (DRBD) used to keep drives synchronized between the primary and secondary hosts in HA configurations
7800	Apache Tomcat	TCP	From the Event Collector to the Extreme Security Console	Real-time (streaming) for events
7801	Apache Tomcat	TCP	From the Event Collector to the Extreme Security Console	Real-time (streaming) for flows

**Table 109: Listening ports that are used by QRadar, services, and components (continued)**

Port	Description	Protocol	Direction	Requirement
7803	Apache Tomcat	TCP	From the Event Collector to the Extreme Security Console	Anomaly detection engine port
8000	Event Collection service (ECS)	TCP	From the Event Collector to the Extreme Security Console	Listening port for specific Event Collection service (ECS).
8001	SNMP daemon port	UDP	External SNMP systems that request SNMP trap information from the Extreme Security Console	UDP listening port for external SNMP data requests.
8005	Apache Tomcat	TCP	None	A local port that is not used by Extreme Security
8009	Apache Tomcat	TCP	From the HTTP daemon (HTTPd) process to Tomcat	Tomcat connector, where the request is used and proxied for the web service
8080	Apache Tomcat	TCP	From the HTTP daemon (HTTPd) process to Tomcat	Tomcat connector, where the request is used and proxied for the web service.
9995	NetFlow data	UDP	From the management interface on the flow source (typically a router) to the QFlow Collector	NetFlow datagram from components, such as routers
10000	Extreme Security web-based, system administration interface	TCP/UDP	User desktop systems to all Extreme Security hosts	Server changes, such as the hosts root password and firewall access
23111	SOAP web server	TCP		SOAP web server port for the event collection service (ECS)
23333	Emulex Fibre Channel	TCP	User desktop systems that connect to Extreme Security appliances with a Fibre Channel card	Emulex Fibre Channel HBAnywhere Remote Management service (elxmgmt)
32004	Normalized event forwarding	TCP	Bidirectional between Extreme Security components	Normalized event data that is communicated from an off-site source or between Extreme Security Event Collectors
32005	Data flow	TCP	Bidirectional between Extreme Security components	Data flow communication port between Extreme Security Event Collectors when on separate managed hosts
32006	Ariel queries	TCP	Bidirectional between Extreme Security components	Communication port between the Ariel proxy server and the Ariel query server

**Table 109: Listening ports that are used by QRadar, services, and components (continued)**

Port	Description	Protocol	Direction	Requirement
32009	Identity data	TCP	Bidirectional between Extreme Security components	Identity data that is communicated between the passive vulnerability information service (VIS) and the Event Collection service (ECS)
32010	Flow listening source port	TCP	Bidirectional between Extreme Security components	Flow listening port to collect data from Extreme Security QFlow Collectors
32011	Ariel listening port	TCP	Bidirectional between Extreme Security components	Ariel listening port for database searches, progress information, and other associated commands
32000-33999	Data flow (flows, events, flow context)	TCP	Bidirectional between Extreme Security components	Data flows, such as events, flows, flow context, and event search queries
40799	PCAP data	TCP	From Juniper Networks SRX Series appliances to Extreme Security	<p>Collecting incoming packet capture (PCAP) data from Juniper Networks SRX Series appliances.</p> <div>  <p><b>Note</b> The packet capture on your device can use a different port. For more information about configuring packet capture, see your Juniper Networks SRX Series appliance documentation</p> </div>
ICMP	ICMP		Bidirectional traffic between the secondary host and primary host in an HA cluster	Testing the network connection between the secondary host and primary host in an HA cluster by using Internet Control Message Protocol (ICMP)

## Searching for ports in use by Extreme Security Console

Use the `netstat` command to determine which ports are in use on the Extreme Security Console or managed host. Use the `netstat` command to view all listening and established ports on the system.

- 1 Using SSH, log in to your Extreme Security Console, as the root user.
- 2 To display all active connections and the TCP and UDP ports on which the computer is listening, type the following command:

```
netstat -nap
```

- 3 To search for specific information from the netstat port list, type the following command:

```
netstat -nap | grep port
```

### Examples

- To display all ports that match 199, type the following command: `netstat -nap | grep 199`
- To display all postgres related ports, type the following command: `netstat -nap | grep postgres`
- To display information on all listening ports, type the following command: `netstat -nap | grep LISTEN`

## Viewing IMQ port associations

You can view port numbers associations for messaging connections (IMQ) to which application services are allocated. To look up the additional port numbers, connect to the localhost by using telnet.



### Note

Random port associations are not static port numbers. If a service is restarted, the ports that generated for a service are reallocated and the service is assigned a new set of port numbers.

- 1 Using SSH to log in to the Extreme Security Console, as the root user.
- 2 To display a list of associated ports for the IMQ messaging connection, type the following command:

```
telnet localhost 7676
```

- 3 If no information is displayed, press the Enter key to close the connection.

# 21 Extreme Security public servers

To provide you with the most current security information, Extreme Networks Security Analytics requires access to a number of public servers and RSS feeds.

## Public servers

This table lists descriptions for the IP addresses or host names that Extreme Security accesses.

**Table 110: Public servers that Extreme Security must access**

IP address or hostname	Description
194.153.113.31	Extreme Networks Security Vulnerability Manager DMZ scanner
194.153.113.32	Extreme Security Vulnerability Manager DMZ scanner
qmmunity.qllabs.com	Extreme Security auto-update server
www.iss.net (Extreme SIEM only)	X-Force Threat Information Center dashboard item
update.xforce-security.com (Extreme SIEM only)	X-Force Threat Feed update server
license.xforce-security.com (Extreme SIEM only)	X-Force Threat Feed licensing server

## RSS feeds for Extreme Security products

The following list describes the requirements for RSS feeds that Extreme Security uses. Copy URLs into a text editor and remove page breaks before pasting into a browser.

**Table 111: RSS feeds**

Title	URL	Requirements
Security Intelligence	<a href="http://feeds.feedburner.com/SecurityIntelligence">http://feeds.feedburner.com/SecurityIntelligence</a>	Extreme Security and an Internet connection
Security Intelligence Vulns / Threats	<a href="http://securityintelligence.com/topics/vulnerabilities-threats/feed">http://securityintelligence.com/topics/vulnerabilities-threats/feed</a>	Extreme Security and an Internet connection
IBM My Notifications	<a href="http://www-945.events.ibm.com/systems/support/myfeed/xmlfeeder.wss?feeder.requid=feeder.create_feed&amp;feeder.feedtype=RSS&amp;feeder.uid=270006EH0R&amp;feeder.subscrid=S14b5f284d32&amp;feeder.subdefkey=swgothor&amp;feeder.maxfeed=25">http://www-945.events.ibm.com/systems/support/myfeed/xmlfeeder.wss?feeder.requid=feeder.create_feed&amp;feeder.feedtype=RSS&amp;feeder.uid=270006EH0R&amp;feeder.subscrid=S14b5f284d32&amp;feeder.subdefkey=swgothor&amp;feeder.maxfeed=25</a>	Extreme Security and an Internet connection
Security News	<a href="http://IP_address_of_QVM_processor:8844/rss/research/news.rss">http://IP_address_of_QVM_processor:8844/rss/research/news.rss</a>	Extreme Networks Security Vulnerability Manager processor is deployed
Security Advisories	<a href="http://IP_address_of_QVM_processor:8844/rss/research/advisories.rss">http://IP_address_of_QVM_processor:8844/rss/research/advisories.rss</a>	Vulnerability Manager processor is deployed
Latest Published Vulnerabilities	<a href="http://IP_address_of_QVM_processor:8844/rss/research/vulnerabilities.rss">http://IP_address_of_QVM_processor:8844/rss/research/vulnerabilities.rss</a>	Vulnerability Manager processor deployed



**Table 111: RSS feeds (continued)**

Title	URL	Requirements
Scans Completed	<a href="http://IP_address_of_QVM_processor:8844/rss/scanresults/completedScans.rss">http://IP_address_of_QVM_processor:8844/rss/scanresults/completedScans.rss</a>	Vulnerability Manager processor is deployed
Scans In Progress	<a href="http://IP_address_of_QVM_processor:8844/rss/scanresults/runningScans.rss">http://IP_address_of_QVM_processor:8844/rss/scanresults/runningScans.rss</a>	Vulnerability Manager processor is deployed

# 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](#).

[A](#) on page 251 [B](#) on page 251 [C](#) on page 251 [D](#) on page 252 [E](#) on page 252 [F](#) on page 252 [G](#) on page 253 [H](#) on page 253 [I](#) on page 253 [K](#) on page 254 [L](#) on page 254 [M](#) on page 254 [N](#) on page 255 [O](#) on page 255 [P](#) on page 255 [Q](#) on page 256 [R](#) on page 256 [S](#) on page 256 [T](#) on page 257 [V](#) on page 257 [W](#) on page 257

## A

<b>accumulator</b>	A register in which one operand of an operation can be stored and subsequently replaced by the result of that operation.
<b>active system</b>	In a high-availability (HA) cluster, the system that has all of its services running.
<b>Address Resolution Protocol (ARP)</b>	A protocol that dynamically maps an IP address to a network adapter address in a local area network.
<b>administrative share</b>	A network resource that is hidden from users without administrative privileges. Administrative shares provide administrators with access to all resources on a network system.
<b>anomaly</b>	A deviation from the expected behavior of the network.
<b>application signature</b>	A unique set of characteristics that are derived by the examination of packet payload and then used to identify a specific application.
<b>ARP</b>	See <a href="#">Address Resolution Protocol</a> .
<b>ARP Redirect</b>	An ARP method for notifying the host if a problem exists on a network.
<b>ASN</b>	See <a href="#">autonomous system number</a> .
<b>asset</b>	A manageable object that is either deployed or intended to be deployed in an operational environment.
<b>autonomous system number (ASN)</b>	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

<b>behavior</b>	The observable effects of an operation or event, including its results.
<b>bonded interface</b>	See <a href="#">link aggregation</a> .
<b>burst</b>	A sudden sharp increase in the rate of incoming events or flows such that the licensed flow or event rate limit is exceeded.

## C

<b>CIDR</b>	See <a href="#">Classless Inter-Domain Routing</a> .
<b>Classless Inter-Domain Routing (CIDR)</b>	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.
<b>client</b>	A software program or computer that requests services from a server.
<b>cluster virtual IP address</b>	An IP address that is shared between the primary or secondary host and the HA cluster.
<b>coalescing interval</b>	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.
<b>Common Vulnerability Scoring System (CVSS)</b>	A scoring system by which the severity of a vulnerability is measured.

<b>console</b>	A display station from which an operator can control and observe the system operation.
<b>content capture</b>	A process that captures a configurable amount of payload and then stores the data in a flow log.
<b>credential</b>	A set of information that grants a user or process certain access rights.
<b>credibility</b>	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.
<b>CVSS</b>	See <a href="#">Common Vulnerability Scoring System</a> .

## D

<b>database leaf object</b>	A terminal object or node in a database hierarchy.
<b>datapoint</b>	A calculated value of a metric at a point in time.
<b>Device Support Module (DSM)</b>	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.
<b>DHCP</b>	See <a href="#">Dynamic Host Configuration Protocol</a> .
<b>DNS</b>	See <a href="#">Domain Name System</a> .
<b>Domain Name System (DNS)</b>	The distributed database system that maps domain names to IP addresses.
<b>DSM</b>	See <a href="#">Device Support Module</a> .
<b>duplicate flow</b>	Multiple instances of the same data transmission received from different flow sources.
<b>Dynamic Host Configuration Protocol (DHCP)</b>	A communications protocol that is used to centrally manage configuration information. For example, DHCP automatically assigns IP addresses to computers in a network.

## E

<b>encryption</b>	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.
<b>endpoint</b>	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.
<b>external scanning appliance</b>	A machine that is connected to the network to gather vulnerability information about assets in the network.

## F

<b>false positive</b>	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).
<b>flow</b>	A single transmission of data passing over a link during a conversation.
<b>flow log</b>	A collection of flow records.
<b>flow sources</b>	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.

<b>forwarding destination</b>	One or more vendor systems that receive raw and normalized data from log sources and flow sources.
<b>FQDN</b>	See <a href="#">fully qualified domain name</a> .
<b>FQNN</b>	See <a href="#">fully qualified network name</a> .
<b>fully qualified domain name (FQDN)</b>	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.
<b>fully qualified network name (FQNN)</b>	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

<b>HA</b>	See <a href="#">high availability</a> .
<b>HA cluster</b>	A high-availability configuration consisting of a primary server and one secondary server.
<b>Hash-Based Message Authentication Code (HMAC)</b>	A cryptographic code that uses a cryptic hash function and a secret key.
<b>high availability (HA)</b>	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.
<b>HMAC</b>	See <a href="#">Hash-Based Message Authentication Code</a> .
<b>host context</b>	A service that monitors components to ensure that each component is operating as expected.

## I

<b>ICMP</b>	See <a href="#">Internet Control Message Protocol</a> .
<b>identity</b>	A collection of attributes from a data source that represent a person, organization, place, or item.
<b>IDS</b>	See <a href="#">intrusion detection system</a> .
<b>Internet Control Message Protocol (ICMP)</b>	An Internet protocol that is used by a gateway to communicate with a source host, for example, to report an error in a datagram.
<b>Internet Protocol (IP)</b>	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 <a href="#">Transmission Control Protocol</a> .
<b>Internet service provider (ISP)</b>	An organization that provides access to the Internet.
<b>intrusion detection system (IDS)</b>	Software that detects attempts or successful attacks on monitored resources that are part of a network or host system.

<b>intrusion prevention system (IPS)</b>	A system that attempts to deny potentially malicious activity. The denial mechanisms could involve filtering, tracking, or setting rate limits.
<b>IP</b>	See <a href="#">Internet Protocol</a> .
<b>IP multicast</b>	Transmission of an Internet Protocol (IP) datagram to a set of systems that form a single multicast group.
<b>IPS</b>	See <a href="#">intrusion prevention system</a> .
<b>ISP</b>	See <a href="#">Internet service provider</a> .

## K

**key file** In computer security, a file that contains public keys, private keys, trusted roots, and certificates.

## L

<b>L2L</b>	See <a href="#">Local To Local</a> .
<b>L2R</b>	See <a href="#">Local To Remote</a> .
<b>LAN</b>	See <a href="#">local area network</a> .
<b>LDAP</b>	See <a href="#">Lightweight Directory Access Protocol</a> .
<b>leaf</b>	In a tree, an entry or node that has no children.
<b>Lightweight Directory Access Protocol (LDAP)</b>	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.
<b>link aggregation</b>	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.
<b>live scan</b>	A vulnerability scan that generates report data from the scan results based on the session name.
<b>local area network (LAN)</b>	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.
<b>Local To Local (L2L)</b>	Pertaining to the internal traffic from one local network to another local network.
<b>Local To Remote (L2R)</b>	Pertaining to the internal traffic from one local network to another remote network.
<b>log source</b>	Either the security equipment or the network equipment from which an event log originates.
<b>log source extension</b>	An XML file that includes all of the regular expression patterns required to identify and categorize events from the event payload.

## M

<b>magistrate</b>	An internal component that analyzes network traffic and security events against defined custom rules.
<b>magnitude</b>	A measure of the relative importance of a particular offense. Magnitude is a weighted value calculated from relevance, severity, and credibility.

## N

<b>NAT</b>	See <a href="#">network address translation</a> .
<b>NetFlow</b>	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.
<b>network address translation (NAT)</b>	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.
<b>network hierarchy</b>	A type of container that is a hierarchical collection of network objects.
<b>network layer</b>	In OSI architecture, the layer that provides services to establish a path between open systems with a predictable quality of service.
<b>network object</b>	A component of a network hierarchy.
<b>network weight</b>	The numeric value applied to each network that signifies the importance of the network. The network weight is defined by the user.

## O

<b>offense</b>	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.
<b>offsite source</b>	A device that is away from the primary site that forwards normalized data to an event collector.
<b>offsite target</b>	A device that is away from the primary site that receives event or data flow from an event collector.
<b>Open Source Vulnerability Database (OSVDB)</b>	Created by the network security community for the network security community, an open source database that provides technical information on network security vulnerabilities.
<b>open systems interconnection (OSI)</b>	The interconnection of open systems in accordance with standards of the International Organization for Standardization (ISO) for the exchange of information.
<b>OSI</b>	See <a href="#">open systems interconnection</a> .
<b>OSVDB</b>	See <a href="#">Open Source Vulnerability Database</a> .

## P

<b>parsing order</b>	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.
<b>payload data</b>	Application data contained in an IP flow, excluding header and administrative information.
<b>primary HA host</b>	The main computer that is connected to the HA cluster.
<b>protocol</b>	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

<b>R2L</b>	See <a href="#">Remote To Local</a> .
<b>R2R</b>	See <a href="#">Remote To Remote</a> .
<b>recon</b>	See <a href="#">reconnaissance</a> .
<b>reconnaissance (recon)</b>	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.
<b>reference map</b>	A data record of direct mapping of a key to a value, for example, a user name to a global ID.
<b>reference map of maps</b>	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.
<b>reference map of sets</b>	A data record of a key mapped to many values. For example, the mapping of a list of privileged users to a host.
<b>reference set</b>	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.
<b>reference table</b>	A table where the data record maps keys that have an assigned type to other keys, which are then mapped to a single value.
<b>refresh timer</b>	An internal device that is triggered manually or automatically at timed intervals that updates the current network activity data.
<b>relevance</b>	A measure of relative impact of an event, category, or offense on the network.
<b>Remote To Local (R2L)</b>	The external traffic from a remote network to a local network.
<b>Remote To Remote (R2R)</b>	The external traffic from a remote network to another remote network.
<b>report</b>	In query management, the formatted data that results from running a query and applying a form to it.
<b>report interval</b>	A configurable time interval at the end of which the event processor must send all captured event and flow data to the console.
<b>routing rule</b>	A condition that when its criteria are satisfied by event data, a collection of conditions and consequent routing are performed.
<b>rule</b>	A set of conditional statements that enable computer systems to identify relationships and run automated responses accordingly.

## S

<b>scanner</b>	An automated security program that searches for software vulnerabilities within web applications.
<b>secondary HA host</b>	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.
<b>severity</b>	A measure of the relative threat that a source poses on a destination.



<b>Simple Network Management Protocol (SNMP)</b>	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).
<b>SNMP</b>	See <a href="#">Simple Network Management Protocol</a> .
<b>SOAP</b>	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.
<b>standby system</b>	A system that automatically becomes active when the active system fails. If disk replication is enabled, replicates data from the active system.
<b>subnet</b>	See <a href="#">subnetwork</a> .
<b>subnet mask</b>	For internet subnetworking, a 32-bit mask used to identify the subnetwork address bits in the host portion of an IP address.
<b>subnetwork (subnet)</b>	A network that is divided into smaller independent subgroups, which still are interconnected.
<b>sub-search</b>	A function that allows a search query to be performed within a set of completed search results.
<b>superflow</b>	A single flow that is comprised of multiple flows with similar properties in order to increase processing capacity by reducing storage constraints.
<b>system view</b>	A visual representation of both primary and managed hosts that compose a system.

## T

<b>TCP</b>	See <a href="#">Transmission Control Protocol</a> .
<b>Transmission Control Protocol (TCP)</b>	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 <a href="#">Internet Protocol</a> .
<b>truststore file</b>	A key database file that contains the public keys for a trusted entity.

## V

<b>violation</b>	An act that bypasses or contravenes corporate policy.
<b>vulnerability</b>	A security exposure in an operating system, system software, or application software component.

## W

<b>whois server</b>	A server that is used to retrieve information about a registered Internet resources, such as domain names and IP address allocations.
---------------------	---------------------------------------------------------------------------------------------------------------------------------------

# Index

---

## A

- about 18
- access category
  - description 203
- accumulator
  - configuring 128
  - description 112, 113
- active directory 25
- admin tab
  - using 14
- Admin tab 13
- aggregated data views
  - deleting 15
  - disabling 15
  - enabling 15
  - managing 15
- application category
  - description 218
- Ariel database
  - right-click actions 74
- asset properties, custom
  - configuring 89
- Asset retention values, overview 76
- audit category
  - description 232
- audit log
  - viewing 190
- audit log file
  - logged actions 191
- audit logs
  - description 190
- authentication
  - LDAP 28
- authentication category
  - description 199
- authorized services
  - about 100
  - adding 101
  - revoking 101
  - token 100
  - viewing 100
- automatic update
  - about 65, 66
  - scheduling 69
- autoupdate log 70

## B

- backing up your information 104
- backup and recovery
  - about 102
  - deleting backup archives 103
  - importing backup archives 103
  - initiating backup 105
  - restoring configuration information 106

- scheduling backups 104
- viewing backup archive 103

## C

- changes
  - deploying 14
- changing 50
- CMT, see content management tool
- collecting log files 46
- commands
  - description 99
- components 131
- configuration 53
- configuring
  - forwarding profiles 158
- content management tool
  - audit details 176, 177
  - custom content item, exporting 172
  - custom content items, exporting multiple 171
  - custom content, exporting all 168
  - custom content, exporting all of a specific type 169
  - custom content, importing 173
  - existing content, updating 175
  - exporting a single custom content item 172
  - exporting all custom content 168
  - exporting all custom content of a specific type 169
  - exporting multiple custom content items 171
  - importing custom content 173
  - searching for custom content 170
  - update 175
- conventions, guide
  - notice icons 7
  - text 8
- CRE category
  - custom rule event, see CRE
  - description 214
- create 21
- create user information source 58
- creating 18, 58
- creating a new store and forward schedule 165
- creating account 23
- custom rules
  - event forwarding 160
- custom rules wizard
  - adding SNMP traps 181
  - configuring SNMP traps 178

## D

- data
  - masking, see obfuscation
  - obfuscation
    - configuring 186
    - decrypting 188
    - description 183

- generating a private/public key pair 184
  - process 183
- restoring 109
- data node
  - archiving data 121
  - save event processor data 122
- Data Node
  - rebalance progress, viewing 121
- deleting 19, 60
- deleting a security profile 23
- deleting a store and forward schedule 166
- deleting backup archives 103
- deploying changes 14
- deployment editor
  - configuring editor preferences 114
  - creating your deployment 114
  - description 112
  - event view 115
  - QRadar components 131
  - requirements 112, 114
  - system view 122
- device access 47
- device management 49
- disabling account 24
- domains
  - creating 137
  - custom properties 141
  - default domain 138, 139
  - domain-aware searches 138, 139
  - overlapping IP addresses 135
  - rules 139
  - segmenting your network 135
  - tagging events and flows 136, 137
  - user-defined domains 138, 139
  - using security profiles 138, 139
- DoS category
  - description 196
- duplicating a security profile 22

## E

- edit 22
- editing 19, 60
- editing a store and forward schedule 165
- email, custom notifications 87
- encryption 122, 123
- event categories
  - description 194
- event category correlation
  - access category 203
  - application category 218
  - audit category 232
  - authentication category 199
  - CRE category 214
  - DoS category 196
  - exploit category
    - description 205
  - high-level categories 194
  - malware category 206

- policy category 212
  - potential exploit category 214
  - recon category 195
  - risk category 233
  - Risk Manager audit category 234
  - SIM Audit events category 216
  - suspicious category 207
  - system category 209
  - unknown category 213
  - User Defined category 215
  - VIS host discovery category 217
- Event Collector
  - about 115, 116
  - configuring 131
- event forwarding
  - configuring 159
  - custom rules 160
- Event Processor
  - about 115, 116
  - configuring 131
- event retention
  - configuring 83
  - deleting 85
  - editing 85
  - enabling and disabling 85
  - managing 84
  - sequencing 84
- event view
  - adding components 116
  - building 115, 116
  - description 112, 113
  - renaming components 121
- events
  - domain creation 137
  - domain tagging 136, 137
  - storing and forwarding 162
  - storing and forwarding events 162
- exploit category 205
- export system details 46
- exporting 43

## F

- firewall access 47
- flow retention
  - deleting 85
  - editing 85
- flow sources
  - domain creation 137
- forwarding destinations
  - adding 157
  - in domain-aware environments 136, 137
  - managing 161
  - specifying properties 158
  - viewing 160
- forwarding normalized events 119
- forwarding profiles
  - configuring 158

## G

glossary 250

## H

hidden updates 70  
high-level categories  
    description 194  
host  
    adding 123  
host context  
    description 112, 113

## I

importing backup archives 103  
index management 90  
initiating a backup 105  
integration workflow 55  
interface roles 49  
introduction 7  
IPv6  
    support and limitations 81, 82

## L

LDAP  
    authentication 28  
LDAP or active directory 25  
license  
    allocating 41  
license allocation 42  
license details  
    viewing 42  
license key 40, 41, 43  
license management 38  
licenses  
    allocating 45  
list of licenses 43  
logged actions  
    audit log file 191

## M

Magistrate  
    configuring 132  
malware category  
    description 206  
manage backup archives 103  
managed host  
    adding 123  
    assigning components 126  
    editing 124  
    removing 125  
managed hosts  
    IPv6 support 81, 82  
management task overview 55  
managing 18, 23, 40, 58

masking, see obfuscation

## N

NAT  
    adding 129  
    editing 129  
    enabling 124  
    removing 129  
    using with QRadar 129  
Net-SNMP 15  
network  
    domains 135  
Network Address Translation. 129  
network administrator 7  
network hierarchy  
    creating 62  
new features  
    version 7.2.5 admin guide overview 11, 12

## O

obfuscation  
    data  
        decrypting 188  
        description 183  
        process 183  
        troubleshooting  
        upgrade 189  
obfuscation\_expressions.xml  
    configuring the obfuscation expression file 186  
obfuscation\_updater.sh  
    configuring obfuscation 186  
off-site source 119  
off-site target 119  
overlapping IP addresses  
    domain segmentation 135  
overview  
    RESTful API 16, 17

## P

parameters  
    description 99  
passwords 50  
payload indexing  
    enabling 91  
payload searches  
    enabling indexes 91  
policy category  
    description 212  
ports  
    searching 247  
ports **usage** 239  
potential exploit category  
    description 214  
public key  
    generating 115

## Q

QRadar SIEM components 131

## R

- RADIUS 25
- RADIUS authentication 25
- RDATE 50
- recon category
  - description 195
- reference data collection
  - creating 98
- reference data collections
  - adding 93
  - adding elements 95
  - deleting 94
  - deleting elements 96
  - editing 93
  - exporting elements 97
  - importing elements 96
  - viewing 93
  - viewing contents 94
- Reference data collections
  - CVS file requirements 96, 97
- reference data utility 98
- reference map 92, 98
- reference map of maps 92, 98
- reference map of sets 92, 98
- reference sets 92
- reference table 92, 98
- restarting 45
- restarting system 45
- RESTful API
  - overview 16, 17
- restored data
  - verifying 110
- restoring
  - data 109
  - troubleshooting restored data 110
- restoring configuration information
  - different IP address 108
  - same IP address 106
- retention buckets 82
- retrieving 59
- reverting a license allocation 42
- right-click menu
  - customizing 73
- right-click menus
  - adding right-click actions 74
- risk category
  - description 233
- Risk Manager audit category
  - description 234
- roles 18, 19
- routing options
  - configuring 161
- routing rules
  - editing 161

rules

- about 92
- domain-aware 139

## S

- scheduling your backup 104
- searching
  - in domain-aware environments 138, 139
- security profile 18, 21-23
- Security profile parameters 36
- security profiles
  - domain privileges 138, 139
- services
  - authorized 100
- setting-up 48
- shutting down 45
- shutting down system 45
- SIM Audit category 216
- SNMP traps
  - adding 181
  - configuration overview 178
  - configuring in customer rules wizard 178
  - configuring trap output 179
  - sending to different host 181
- source
  - off-site 119
- SSL certificate
  - configuring 33
- SSL certificates
  - replacement overview 79
  - replacing 79
- store and forward
  - creating a new schedule 165
  - deleting a schedule 166
  - editing a schedule 165
  - viewing the schedule list 163
- store user information 61
- suspicious category
  - description 207
- syslog
  - forwarding 157
- system 25, 45
- system and license management
  - log file collection 46
- system authentication 25
- system category
  - description 209
- system details 43
- system health 44
- system management 38, 43
- system settings 73
- system setup 47
- system time 50
- system view
  - adding a host 123
  - assigning components 126
  - description 112, 113
  - Host Context 126

managed host 125  
managing 122

## T

TACACS 25  
TACACS authentication 25  
target  
    encryption 119  
    off-site 119  
thresholds 86  
time server configuration 50  
Tivoli Directory Integrator server 53, 56  
TLS certificate  
    configuring 33  
troubleshooting  
    restored data 110  
    upgrade  
        obfuscated data 189  
trusted root  
    SSL certificates 79

## U

undo license allocation 42  
unknown category  
    description 213  
update 15  
update history 70  
updates  
    scheduling 68  
upload 41  
user 24  
user accounts 23  
User Defined category  
    description 215  
user details  
    user 15  
User Details window 37  
user information 54, 61  
user information source 55, 58  
user information sources 53, 58–60  
user interface 13  
user management 18, 36  
user management window parameters 36  
user management window toolbar 36  
user role 18  
user role management 34  
user roles 18  
users 18, 23, 24

## V

variable binding  
    SNMP traps 179  
view backup archives 103  
viewing backup archives 103  
viewing the schedule list 163  
VIS host discovery category

description 217

## W

web browsers  
    supported versions 13  
what's new  
    version 7.2.5 admin guide overview 11, 12