Extreme Networks SIEM Administration Guide

9034878

Published July 2015

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

Introduction to Extreme SIEM product administration

Administrators use Extreme SIEM to manage dashboards, offenses, log activity, network activity, assets, and reports.

Intended audience

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

Statement of good security practices

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

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

Conventions

This section discusses the conventions used in this guide.

Text Conventions

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

Table 1: Notice Icons

Icon	Notice Type	Alerts you to...
☞	Tip	Helpful tips for using the product.
📝	Note	Important features or instructions.
⚠	Caution	Risk of personal injury, system damage, or loss of data.
⚠	Warning	Risk of severe personal injury.
New	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 italicized type	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 and flow collectors, log sources, log source groups, flow sources, 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.

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

Administrators use the Admin tab in Extreme SIEM to manage dashboards, offenses, log activity, network activity, assets, and reports.

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

Supported web browsers

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

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

The following table lists the supported versions of web browsers.

Table 3: Supported web browsers for Extreme Security products

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

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 126.
Deploy Changes	Deploys any configuration changes from the current session to your deployment. For more information, see Deploying changes on page 15.
Advanced	The Advanced menu provides the following options: Clean SIM Model - Resets the SIM module. See Resetting SIM on page 16. Deploy Full Configuration - Deploys all configuration changes. When you deploy the full configuration, Extreme Security restarts all services. Data collection for events and flows stops until the deployment completes. For more information, see Deploying changes on page 15.

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.

> Important
>
> When you click Deploy Full Configuration, Extreme SIEM restarts all services, which result in a gap in data collection until deployment completes.

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 and flows 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 *Users Guide* for your product.

3. Click **Save**.

Resetting SIM

Use the **Admin** to reset the SIM module. You can now remove all offense, source IP address, and destination IP address information from the database and the disk.

This option is useful after you tune your deployment to avoid receiving any additional false positive information.

The SIM reset process can take several minutes, depending on the amount of data in your system. If you attempt to move to other areas of the Extreme SIEM user interface during the SIM reset process, an error message is displayed.

1. Click the **Admin** tab.
2. From the **Advanced** menu, select **Clean SIM Model**.
3. Read the information on the **Reset SIM Data Module** window.

4 Select one of the following options.

Option	Description
Soft Clean	Closes all offenses in the database. If you select the **Soft Clean** option, you can also select the **Deactivate all offenses** check box.
Hard Clean	Purges all current and historical SIM data, which includes offenses, source IP addresses, and destination IP addresses.

5 If you want to continue, select the **Are you sure you want to reset the data model?** check box.

6 Click **Proceed**.

7 When the SIM reset process is complete, click **Close**.

8 When the SIM reset process is complete, reset your browser.

Monitoring systems with SNMP

Monitoring of appliances through SNMP polling.

Extreme SIEM 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, report charts, and anomaly rules 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 and flow counts instead of average counts over time.

3 User management

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 Extreme SIEM, you must create user accounts for all users that require access to Extreme SIEM. 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 you create:

- User role - Determines the privileges that the user is granted to access functions and information in Extreme SIEM. Extreme SIEM includes two default user roles: 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 access to. Extreme SIEM 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 Extreme SIEM. 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 35.
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 35.
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 and flows in the Network 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 and which flows are displayed in the Network Activity tab.
- Network Only - This option restricts the user to view only events and flows 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 and flows 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 and flows 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.

Extreme SIEM 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 21.
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. Extreme SIEM 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 21.
    - If no user accounts are assigned to this security profile, the security profile is successfully deleted. Go to Deleting a user role on page 21.
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.

Extreme SIEM 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 63 Configuring the Console settings on page 94.

An administrative user can access Extreme SIEM 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.

Extreme SIEM 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, Extreme SIEM 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, Extreme SIEM 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. Extreme SIEM 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 Extreme Security. For more information, see your server documentation
- Ensure that the server has the appropriate user accounts and privilege levels to communicate with Extreme Security. For more information, see your server documentation.
- Ensure that the time of the authentication server is synchronized with the time of the Extreme Security server. For more information about setting time, see Set up Extreme Security on page 63.
- 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 Extreme SIEM 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 SIEM 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, ldaps://`host`:`port`.
LDAP Context	Type the LDAP context you want to use, for example, DC=QRADAR,DC=INC.
LDAP Domain	Type the LDAP context you want to use, for example, DC=QRADAR,DC=INC.
LDAP Domain	Type the domain that you want to use, for example qradar.inc.

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/qradar/conf/trusted_certificates` directory on your Extreme Security console. For more information about configuring the certificates, see Configuring SSL or TLS certificates on page 34.

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 6: 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, `ldap://<host_name>:<port>` or `ldap://<ip_address>:<port>`.
SSL connection	If SSL encryption is enabled, the value in the Server URL field must specify a secure connection, for example, `ldaps://secureldap.mydomain.com:636`.
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.
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 `ibm.com`, the base DN value would be `cn=Users,dc=ibm,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 ibm.com, the Login DN would be `cn=admin,dc=ibm,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 `ibm.com` and Repository_2 is configured to use domain `ibm.ca.com`. When a user tries to log in, they must specify the domain name in the user name field, such as `ibm.ca.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 7: 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 8: 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, offenses, or assets.

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=(&(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.q1labs.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 and Offenses tabs, or hover over the Last User field on the Assets tab 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.

Table 9: Description of User Role Management window parameters

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>User Role name</td><td>A unique name for the role.</td></tr>
<tr><td>Admin</td><td>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></td></tr>
<tr><td>Offenses</td><td>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></td></tr>
<tr><td>Log Activity</td><td>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></td></tr>
</table>

Table 9: Description of User Role Management window parameters (continued)

Parameter	Description
Assets	Note This permission is displayed only if Extreme Networks Security Vulnerability Manager is installed on your system. Grants access to the function in the Assets tab. You can grant specific permissions: Perform VA Scans — Grants permission to complete vulnerability assessment scans. For more information about vulnerability assessment, see the *Managing Vulnerability Assessment guide*. 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 *Managing Vulnerability Assessment guide.*
Network Activity	Grants access to all the functions in the Network Activity tab. You can grant specific access to the following permissions: 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. User Defined Flow Properties — Grants permission to create custom flow properties. 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. View Flow Content — Grants permission to access to flow data.
Reports	Grants permission to access to all the functions in the Reports tab. You can grant users-specific permissions: Distribute Reports via Email — Grants permission to distribute reports through email. Maintain Templates — Grants permission to edit report templates.
Vulnerability Manager	Grants permission to Extreme Security Vulnerability Manager function. Extreme Networks Security Vulnerability Manager must be activated. For more information, see the *Extreme Networks Security Vulnerability Manager User Guide*.
Forensics	Grants permission to Extreme Security Incident Forensics capabilities. Create cases in Incident Forensics — Grants permission to create cases for collections of imported document and pcap files.

Table 9: Description of User Role Management window parameters (continued)

Parameter	Description
IP Right Click Menu Extensions	Grants permission to options added to the right-click menu.
Platform Configuration	Grants permission to Platform Configuration services. 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 10: 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: • 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 11: 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 12: 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 25.
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 13: 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: • 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: • 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 19.
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 21.

4 System and licenses management

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. QFlow and 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 14: 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 42.

Table 14: System and License Management toolbar functions (continued)

Function	Description
Actions (License)	If you select Licenses from the Display list box in the Deployment Details pane, the following functions are available on the Actions menu: 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.
Actions (System)	If you select Systems from the Display list box in the Deployment Details pane, the following functions are available on the Actions menu: • 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 44. • Revert Allocation - Select this option to undo staged license changes. The configuration reverts to the last deployed license allocation. 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. • 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 48. • 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 46. • Restart System - Select a system, and then select this option to restart the system. For more information, see Restarting a system on page 46.

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 15: 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 15: 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: • 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 your license allows.
Flow Rate Limit	Displays the flow rate limit 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 42
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 and flows 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 46

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.

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 system to a license.

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 16: 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: • 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.
Flow Rate Limit	Displays the flow 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 43.
- Click Upload Licenses to upload a license. See Uploading a license key on page 42.
- Click Allocate License to System on the toolbar to assign a license. See Allocating a system to a license on page 46.

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, events per second (EPS) and flows per second (FPS).

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 the Extreme SIEM, 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 Extreme SIEM deployment. To help distribute processing, you can add Extreme Security Event Collectors, or Extreme Security Flow Processors, 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 Incident Forensics in your deployment, you can add a Extreme Security Incident Forensics managed host. For more information, see the *IBM® Security QRadar® Incident Forensics Installation Guide*

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 want risk management, you need to install Extreme Networks Security Risk Manager and then 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 131

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.

If you change the **External Flow Source Monitoring Port** parameter in the QFlow configuration, you must also update your firewall access configuration. For more information about QFlow configuration, see Deployment editor on page 126.

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 IBM 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: • **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. Extreme SIEM uses this mail server to distribute alerts and event messages. To use the mail server that Extreme SIEM 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:
   1. Click the **Change time zone** tab.
   2. From the **Change timezone to** list box, select the time zone in which this managed host is located.
   3. Click **Save**.
10. Configure the time server:
    1. Click the **Time server sync** tab.

       Configure the following parameters:

Table 17: 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: • 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

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

Extreme SIEM 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 Extreme SIEM 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 18: 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.	• 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
IBM® 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 IBM® Security Access Manager (ISAM) documentation.	• name_in_rgy • first-name • last-name • account_valid • password_valid
IBM® 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 IBM® 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 IBM® Security Integration Manager (ISIM) documentation.	• 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 Extreme SIEM 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 SIEM.

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 59.
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 57.
2. Create and manage user information sources. See Creating and managing user information source on page 59.

3 Collect user information. See Collecting user information on page 62.

Configuring the Tivoli® Directory Integrator Server

For Extreme SIEM 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 19: Certification configuration parameters

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

1 Install Tivoli® Directory Integrator on a non-Extreme Securityhost. 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 SIEM 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 SIEM 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 encryps the first time that you start Tivoli® Directory Integrator.

10 Use one of the following scripts to start the Tivoli® Directory Integrator:

- QradarIAM.sh for Linux™
- QradarIAM.bat for Microsoft™ Windows

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 57.

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 20: Supported user interface property values

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

Table 20: 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 Extreme SIEM 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 59.

   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 59.

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 on the Extreme SIEM 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.

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 date 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 55.

6 Set up Extreme Security

Use the features on the Admin tab to set up Extreme SIEM.

You can configure your network hierarchy, automatic updates, system settings, event and flow retention buckets, `system notifications,` console settings, offense close reasons, 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.

If your deployment processes more than 600,000 flows, then you can create multiple top-level groups.

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 21: 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 10.10.1.4/32 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 22: 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 23: 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

Table 23: Acceptable CIDR values (continued)

CIDR Length	Mask	Number of Networks	Hosts
/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
/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 on page 66

Extreme Security considers all networks in the network hierarchy as local. Keep the network hierarchy up to date to prevent false offenses.

Defining your network hierarchy

Extreme Security considers all networks in the network hierarchy as local. Keep the network hierarchy up to date to prevent false offenses.

The relevance of an offense, which is a security or compliance breach, indicates the importance of a destination. Less important areas of the network have a lower relevance. Extreme Security determines the relevance of an offense by the weight of the networks and assets.

The weight of a network object is indicated by a numeric value from 0 through 99, with 99 being the highest, and 0 being the lowest. This weight sets the importance of the network object in relation to the other network objects.

Network objects are a container for CIDR addresses. Any IP address that is covered by a CIDR range in the network hierarchy is considered a local address. Any IP address that is not defined in a network objects CIDR range is considered a remote IP address. A CIDR can belong only to one network object, however subsets of a CIDR range can belong to another network object. Network traffic matches the most exact CIDR. A network object can have multiple CIDR ranges assigned to it.

1. Click the Admin tab.
2. On the navigation menu, click System Configuration.
3. Click Network Hierarchy.
4. From the menu tree on the Network Views window, select the area of the network in which you want to work.
5. To add network objects, follow these steps:
   a. Click Add and type a unique name and description for the object.
   b. From the Group list, select the group in which you want to add the new network object.
   c. To add a group, click the icon beside the Group list and type a name for the group.
   d. Type or select the weight of the object.
   e. Type a CIDR range for this object and click Add.
   f. Click Create.
   g. Repeat the steps for all network objects.
6. Click Edit or Delete to work with existing network objects.

Related Links

Acceptable CIDR values on page 64

Extreme Security accepts specific CIDR values.

Automatic updates

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

Extreme Security uses system configuration files to provide useful characterizations of network data flows.

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:

IBM Fix Central (http://www.ibm.com/support/fixcentral).

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 126.

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.

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 72

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 71.

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

Table 24: Check for Updates toolbar functions

Function	Description
Hide	Select one or more updates, and then click Hide to remove the selected updates from the Check for Updates page. You can view and restore the hidden updates on the Restore Hidden Updates page. For more information, see Restoring hidden updates on page 72.
Install	You can manually install updates. When you manually install updates, the installation process starts within a minute. For more information, see Manually installing automatic updates on page 71.
Schedule	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 Scheduling an update on page 70.
Unschedule	You can remove preconfigured schedules for manually installing updates on your Console. For more information, see Scheduling an update on page 70.
Search By Name	You can locate a specific update by name.
Next Refresh	This counter displays the amount of time until the next automatic refresh. The list of updates on the Check for Updates page automatically refreshes every 60 seconds. The timer is automatically paused when you select one or more updates.
Pause	Pauses the automatic refresh process. To resume automatic refresh, click Play.
Refresh	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.q1labs.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 IBM 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 67

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 -zxf 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 -zxf 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 system settings.

On the System Settings window, you can configure the following parameters:

Table 25: System Settings window parameters

Parameter	Description
System Settings	
Administrative Email Address	The email address of the designated system administrator. The default email address is root@localhost.
Alert Email From Address	The email address from which you want to receive email alerts. This address is displayed in the From field of the email alerts. A valid address is required by most email servers. The default email address is root@<hostname.domain>.
Email Locale	The locale to be used for language preferences and system alert email messages, including emails that are triggered in response to a rule. The default setting is English.
Resolution Interval Length	The resolution interval length determines at what interval the QFlow Collector and Event Collectors send bundles of information to the Console. If you select the 30-seconds option, results display on the Extreme Security user interface as the data enters the system. However, with shorter intervals, the volume of time series data is larger and the system might experience delays in processing the information.
Delete Root Mail	Root mail is the default location for host context messages.
Temporary Files Retention Period	The period that you want the system to retain temporary files. The default storage location for temporary files is the `/store/tmp` directory.
Asset Profile Query Period	The period for an asset search to process before a timeout occurs.
Coalescing Events	The coalesce log settings for events. Select Yes to enable log sources to coalesce, or bundle, events. This setting applies to all new log sources that you add. For log sources that you previously added or to change an individual log source, you must edit the Coalescing Event parameter in the log source configuration.
Store Event Payload	Log sources can store event payload information. This value applies to all log sources. However, if you want to alter this value for a specific log source, edit the Event Payload parameter in the log source configuration. For more information, see the *Extreme Networks Security Managing Log Sources Guide* users guide.
Global Iptables Access	The IP addresses of non-Console systems that do not have iptables configuration to which you want to enable direct access. To enter multiple systems, type a comma-separated list of IP addresses.

Table 25: System Settings window parameters (continued)

Parameter	Description
Syslog Event Timeout (minutes)	The amount of time that the status of a syslog device is recorded as an error if no events are received within the timeout period. The status is displayed on the Log Sources window.
Partition Tester Timeout (seconds)	The amount of time for a partition test to perform before a timeout occurs.
Max Number of TCP Syslog Connections	The maximum number of Transmission Control Protocol (TCP) syslog connections you want to allow your system.
Export Directory	The location where offense, event, and flow exports are stored. The default location is `/store/exports`.
Display Country/Region Flags	If geographic information is available for an IP address, the country or region is visually indicated by a flag. You can select No from this list box disable this feature.
Database Settings	
User Data Files	The location of the user profiles. The default location is `/store/users`.
Accumulator Retention - Minute-By-Minute	The period that you want to retain minute-by-minute data accumulations. Every 60 seconds, the data is aggregated into a single data set.
Accumulator Retention - Hourly	The period that you want to retain hourly data accumulations. At the end of every hour, the minute-by minute data sets are aggregated into a single hourly data set.
Accumulator Retention - Daily	The period that you want to retain daily data accumulations. At the end of every day, the hourly data sets are aggregated into a single daily data set.
Payload Index Retention	The amount of time you want to store payload indexes.
Offense Retention Period	The period that you want to retain closed offense information. The default setting is 30 days. The minimum is 1 day and the maximum is 2 years. After the offense retention period elapses, closed offenses are purged from the database. Offenses can be retained indefinitely if they are not closed or inactive, and they are still receiving events. The magistrate automatically marks an offense as Inactive if the offense has not received an event for 5 days. This 5-day period is known as the dormant time. If an event is received during the dormant time, the dormant time is reset back to zero. When an offense is closed either by you (Closed) or the magistrate (Inactive), the Offense Retention Period setting is applied.
Attacker History Retention Period	From the list box, select the amount of time that you want to store the attacker history.
Target Retention Period	From the list box, select the amount of time that you want to store the target history.
Ariel Database Settings	
Flow Data Storage Location	The location that you want to store the flow log information. The default location is `/store/ariel/flows`.
Log Source Storage Location	The location where you want to store the log source information. The default location is `/store/ariel/events`.
Search Results Retention Period	The amount of time you want to store search results.

Table 25: System Settings window parameters (continued)

Parameter	Description
Reporting Max Matched Results	The maximum number of results you want a report to return.
Command Line Max Matched Results	The maximum number of results you want the AQL command line to return.
Web Execution Time Limit	The maximum amount of time, in seconds, you want a query to process before a timeout occurs.
Reporting Execution Time Limit for Manual Reports	The maximum amount of time, in seconds, you want a reporting query to process before a timeout occurs.
Command Line Execution Time Limit	The maximum amount of time, in seconds, you want a query in the AQL command line to process before a timeout occurs.
Web Last Minute (Auto refresh) Execution Time Limit	The maximum amount of time, in seconds, you want an auto refresh to process before a timeout occurs.
Flow Log Hashing	Stores a hash file for every stored flow log file. Select Yes to enable logging.
Event Log Hashing	Stores a hash file for every stored event log file. Select Yes to enable logging.
HMAC Encryption	This parameter only displays when the Event Log Hashing or Flow Log Hashing system setting is enabled. Select Yes to allow Extreme Security to encrypt the integrity hashes on stored event and flow log files.
HMAC Key	The key that you want to use for HMAC encryption. The key must be unique.
Verify	This parameter only displays when the HMAC Encryption system setting is enabled. Retype the key that you want to use for HMAC encryption. The key must match the key that you typed in the HMAC Key field.

Table 25: System Settings window parameters (continued)

Parameter	Description
Hashing Algorithm	You can use a hashing algorithm for database integrity. Extreme Security uses the following hashing algorithm types: • Message-Digest Hash Algorithm - Transforms digital signatures into shorter values called Message-Digests (MD). • Secure Hash Algorithm (SHA) Hash Algorithm - Standard algorithm that creates a larger (60 bit) MD. If the HMAC Encryption parameter is disabled, the following options are available: • MD2 - Algorithm that is defined by RFC 1319. • MD5 - Algorithm that is defined by RFC 1321. • SHA-1 - Algorithm that is defined by Secure Hash Standard (SHS), NIST FIPS 180-1. This is the default setting. • SHA-256 - Algorithm that is defined by the draft Federal Information Processing Standard 180-2, SHS. SHA-256 is a 255-bit hash algorithm that is intended for 128 bits of security against security attacks. • SHA-384 - Algorithm that is defined by the draft Federal Information Processing Standard 180-2, SHS. SHA-384 is a bit hash algorithm, created by truncating the SHA-512 output. • SHA-512 - Algorithm that is defined by the draft Federal Information Processing Standard 180-2, SHS. SHA-512 is a bit hash algorithm that is intended to provide 256 bits of security. If the HMAC Encryption parameter is enabled, the following options are available: • HMAC-MD5 - An encryption method that is based on the MD5 hashing algorithm. • HMAC-SHA-1 - An encryption method that is based on the SHA-1 hashing algorithm. • HMAC-SHA-256 - An encryption method that is based on the SHA-256 hashing algorithm. • HMAC-SHA-384 - An encryption method that is based on the SHA-384 hashing algorithm. • HMAC-SHA-512 An encryption method that is based on the SHA-512 hashing algorithm.
Transaction Sentry Settings	
Transaction Max Time Limit	A transaction sentry detects unresponsive applications using transaction analysis. If an unresponsive application is detected, the transaction sentry attempts to return the application to a functional state. The length of time you want the system to check for transactional issues in the database.
Resolve Transaction on Non-Encrypted Host	The transaction sentry can resolve all error conditions that are detected on the Console or non-encrypted managed hosts. If you select No, the conditions are detected and logged but you must manually intervene and correct the error.
Resolve Transaction on Encrypted Host	The transaction sentry can resolve all error conditions that are detected on the encrypted managed host. If you select No, the conditions are detected and logged but you must manually intervene and correct the error.
SNMP Settings	
SNMP Version	The version of SNMP that you want to use. Disable this setting if you do not want SNMP responses in the Extreme Security custom rules engine.

Table 25: System Settings window parameters (continued)

Parameter	Description
SNMPv2c Settings	
Destination Host	The IP address to which you want to send SNMP notifications.
Destination Port	The port number to which you want to send SNMP notifications.
Community	The SNMP community, such as public.
SNMPv3 Settings	
Destination Host	The IP address to which you want to send SNMP notifications.
Destination Port	The port to which you want to send SNMP notifications.
Username	The name of the user you want to access SNMP-related properties.
Security Level	The security level for SNMP.
Authentication Protocol	The algorithm that you want to use to authenticate SNMP traps.
Authentication Password	The password that you want to use to authenticate SNMP traps.
Privacy Protocol	The protocol that you want to use to decrypt SNMP traps.
Privacy Password	The password that is used to decrypt SNMP traps.
Embedded SNMP Daemon Settings	
Enabled	Enables access to data from the SNMP Agent using SNMP requests. After you enable the embedded SNMP daemon, you must access the host that is specified in the Destination Host parameter and type `qradar` in the Username field. A password is not required. The location where you configure a destination host to communicate with QRadar® SIEM can vary depending on the vendor host. For more information on configuring your destination host to communicate with Extreme Security, see your vendor documentation.
Daemon Port	The port that you want to use for sending SNMP requests.
Community String	The SNMP community, such as public. This parameter applies only if you are using SNMPv2 and SNMPv3.
IP Access List	The systems that can access data from the SNMP agent using an SNMP request. If the Enabled option is set to Yes, this option is enforced.
IF-MAP Client/Server Settings	
IF-MAP Version	The version of IF-MAP that you require. The Interface For Metadata Access Points (IF-MAP) rule response enables Extreme SIEM to publish alert and offense data derived from events, flows, and offense data on an IF-MAP server. If this setting is disabled, the other IF-MAP Client/Server settings are not displayed.
Server Address	The IP address of the IF-MAP server.
Basic Server Port	The port number for the basic IF-MAP server.
Credential Server Port	The port number for the credential server. .
Authentication	The type of authentication that you require. Before you can configure IF-MAP authentication, you must configure your IF-MAP server certificate.

Table 25: System Settings window parameters (continued)

Parameter	Description
Key Password	The key password to be shared between the IF-MAP client and server. This setting is displayed only when you select the Mutual option for the Authentication setting.
Username	The user name that is required to access the IF-MAP server. This setting is displayed only when you select the Basic option for the Authentication setting.
User Password	The password that is required to access the IF-MAP server. This setting is displayed only when you select the Basic option for the Authentication setting.
Asset Profile Settings This pane is only displayed if Extreme Networks Security Vulnerability Manager is installed on your system.	
Asset Profile Retention Period	The period, in days, that you want to store the asset profile information. The Use Advanced setting enables Extreme Security to apply advanced, granular database retention logic to asset data. The granular database retention logic allows you to select from a variety of different settings. If you want to apply one retention period to all asset data, you can configure this system setting.
Enable DNS Lookups for Host Identity	Enables Extreme Security to run Domain Name System (DNS) lookups for host identity.
Enable WINS Lookups for Host Identity	Enables Extreme Security to run Windows™ Internet Name Service (WINS) lookups for host identity.
Asset Profile Reporting Interval	The interval, in seconds, that the database stores new asset profile information.

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 and flows stops until the deployment completes.

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 26: 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.
DNS and NetBIOS Hostnames	120 days	by default, user-supplied hostnames are retained until they are deleted manually.
Asset Properties	120 days	By default, user-supplied IP Addresses are retained until they are deleted manually. the asset properties this value can affect are: • Given Name • Unified Name • Weight • Description • Business Owner • Business Contact • Technical Owner • Technical Contact • Location • Detection Confidence • Wireless AP • Wireless SSID • Switch ID • Switch Port ID • CVSS Confidentiality Requirement • CVSS Integrity Requirement • CVSS Availability Requirement • CVSS Collateral Damage Potential • Technical User • User Supplied OS • OS Override Type • OS Override Id • Extended • Legacy (Pre-7.2) Cvss Risk • VLAN • Asset Type

Table 26: Asset components (continued)

Asset component	Default retention (in days)	Notes
Asset Products	120 days	By default, user-supplied products are retained until they are deleted manually. Asset products include the following: • Asset OS • Asset Installed Applications • Products that are associated with open asset ports
Asset "Open" Ports	120 days	
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/qradar/conf/trusted_certificateschmod 644 /opt/qradar/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 Extreme Security, 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 85

Deploying Extreme Security in IPv6 or mixed environments on page 86

IPv6 addressing limitations on page 86

Extreme Security components that support IPv6 addressing

The following Extreme Security components support IPv6: addressing.

Network Activity tab

Because IPv6 Source Address and IPv6 Destination Address 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).

To save space and indexing in an IPv4 or IPv6 source environment, extra IP address fields are not stored or displayed. In a mixed IPv4 and IPv6 environment, a flow record contains both IPv4 and IPv6 addresses.

IPv6 addresses are supported for both packet data, including sFlow, and NetFlow V9 data. However, older versions of NetFlow might not support IPv6.

Log Activity tab	Because IPv6 Source Address and IPv6 Destination Address 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). 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 *Extreme Networks Security Log Sources User Guide*.
Searching, grouping, and reporting on IPv6 fields	You can search events and flows by using IPv6 parameters in the search criteria. You can also group and sort event and flow records that are based on IPv6 parameters. You can create reports that are based on data from IPv6-based searches.
Custom rules	The following custom rule to support IPv6 addressing was added: SRC/DST IP = IPv6 Address IPv6-based building blocks are available in other rules.
Deployment editor	The deployment editor supports IPv6 addresses.
Device support modules (DSMs)	DSMs can parse IPv6 source and destination address from event payloads.

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.

Flow sources, such as NetFlow and sFlow, are accepted from IPv4 and IPv6 addresses. Event sources, such as syslog and SNMP, are accepted from IPv4 and IPv6 addresses. You can disable superflows and flow bundling in an IPv6 environment.

Restriction

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 Extreme Security 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, flows, and vulnerability data for IPv4 hosts.
- No host profile test in custom rules for IPv6 addresses.
- No specialized indexing or optimization of IPv6 addresses.
- No IPv6-based sources and destinations for offenses

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 and flows that match custom filter requirements. As Extreme Security receives events and flows, each event and flow is compared against retention bucket filter criteria. When an event or flow 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 and Flow Retention windows. 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 and Flow Retention windows provide a default retention bucket and 10 unconfigured retention buckets. Until you configure a retention bucket, all events or flows are stored in the default retention bucket.

The Event Retention and Flow Retention windows provide the following information for each retention bucket:

Table 27: 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 Filters 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 28: 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 or Flow Retention icon.
4. Double-click the first available retention bucket.
5. Configure the following parameters:

Parameter	*Description*
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 *Delete data in this bucket* 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.

Parameter	*Description*
Delete data in this bucket	Select a deletion policy. Select When storage space is required if you want data that matches the *Keep data placed in this bucket for* 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. Select Immediately after the retention period has expired if you want data to be deleted immediately on matching the Keep data placed in this bucket for parameter. The data is deleted at the next scheduled disk maintenance process, regardless of free disk space or compression requirements. When storage is required, only data that matches the Keep data placed in this bucket for parameter are deleted.
Description	Type a description for the retention bucket.
Current Filters	Configure your filters. From the first list, select a parameter you want to filter for. For example, Device, Source Port, or Event Name. 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. In the text field, type specific information related to your filter and then click Add Filter. The filters are displayed in the Current Filters text box. You can select a filter and click Remove Filter to remove a filter from the Current Filter text box.

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 and Flow Retention windows. 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 or Flow 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 Click the Flow Retention icon.
6 Select the retention bucket you want to edit, and then click Edit.
7 Edit the parameters. For more information see, Configuring retention buckets on page 87.
8 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 or flow retention.

When you disable a bucket, any new events or flows that match the requirements for the disabled bucket are stored in the next bucket that matches the event or flow 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 Click the Flow Retention icon.
6 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 or flows contained in the retention bucket are not removed from the system, only the criteria defining the bucket is deleted. All events or flows are maintained in storage.

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 Click the Flow Retention icon.
6 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 29: 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
Greater Than	An alert occurs if the parameter value exceeds the configured value.
Less Than	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 Extreme Security, 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 or flow 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 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 Extreme Security 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.

   Restriction
   Although you can add multiple template elements, you can set the `Active property` to `True` in only one event and one flow template type.
7. Edit the contents of the `<template></template>` element:
   a. Specify the template type by using the following XML property:

      `<templatetype></templatetype>`

      The possible values are event or flow. 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 Extreme Security.

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 and flows stops until the deployment completes.

Table 30: 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
Qid	DstMACAddress	OutputIFIndexList
Category	DstPostNATIPAddress	AppId
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

Table 30: Accepted Notification Parameters (continued)

Common Parameters	Event Parameters	Flow Parameters
StartTime		InputIFIndex
Duration		OutputIFIndex
StopTime		FirstPacketTime
EventCount		LastPacketTime
SourceV6		TotalSourceBytes
DestinationV6		TotalDestinationBytes
UserName		TotalSourcePackets
DestinationNetwork		TotalDestinationPackets
SourceNetwork		SourceQOS
Severity		DestinationQOS
CustomPropertiesList		SourcePayload

Configuring the Console settings

The Console provides real-time views, reports, alerts, and in-depth investigation of network traffic and security threats. You can configure the Console to manage distributed Extreme Security deployments.

The following table describes the Console settings:

Table 31: Console settings

Settings	Description
Console Settings	
ARP - Safe Interfaces	Type the interfaces that you want to be excluded from ARP resolution activities.
Results Per Page	Type the maximum number of results you want to display on the user interface. This parameter applies to the **Offenses**, **Log Activity**, **Assets**, **Network Activity**, and **Reports** tabs. For example, if the **Default Page Size** parameter is configured to 50, the **Offenses** tab displays a maximum of 50 offenses.
Authentication Settings	
Persistent Session Timeout (in days)	Type the length of time, in days, that a user system is persisted.
Maximum Login Failures	Type the number of times a login attempt can fail.
Login Failure Attempt Window (in minutes)	Type the length of time during which a maximum number of login failures can occur before the system is locked.
Login Failure Block Time (in minutes)	Type the length of time that the system is locked if the maximum login failures value is exceeded.
Login Host Whitelist	Type a list of hosts who are exempt from being locked out of the system. Enter multiple entries using a comma-separated list.
Inactivity Timeout (in minutes)	Type the amount of time that a user is automatically logged out of the system if no activity occurs.

Table 31: Console settings (continued)

Settings	Description
Login Message File	Type the location and name of a file that includes content you want to display on the Extreme Security login window. The contents of the file are displayed below the current login window. The login message file must be located in the `/opt/qradar/conf` directory on your system. This file will be in text format.
Event Permission Precedence	From the list box, select the level of network permissions you want to assign to users. This parameter affects the events that are displayed on the Log Activity tab. The options include: • Network Only - A user must have access to either the source network or the destination network of the event to have that event display on the Log Activity tab. • Devices Only - A user must have access to either the device or device group that created the event to have that event display on the Log Activity tab. • Networks and Devices - A user must have access to both the source or the destination network and the device or device group to have an event display on the Log Activity tab. • None - All events are displayed on the Log Activity tab. Any user with Log Activity role permissions is able to view all events. For more information about managing users, see User management on page 19.
DNS Settings	
Enable DNS Lookups for Asset Profiles	From the list box, select whether you want to enable or disable the ability for Extreme Security to search for DNS information in asset profiles. When enabled, this information is available in the right-click menu for the IP address or host name that is located in the Host Name (DNS Name) field in the asset profile.
Enable DNS Lookups for Host Identity	From the list box, select whether you want to enable or disable the ability for Extreme Security to search for host identity information. When enabled, this information is available in the right-click menu for any IP address or asset name.
WINS Settings	
WINS Server	Type the location of the Windows Internet Naming Server (WINS) server.
Reporting Settings	
Report Retention Period	Type the period, in days, that you want the system to maintain reports.
Data Export Settings	
Include Header in CSV Exports	From the list box, select whether you want to include a header in a CSV export file.
Maximum Simultaneous Exports	Type the maximum number of exports you want to occur at one time.

1. Click the Admin tab.
2. On the navigation menu, click System Configuration.
3. Click the Console icon.
4. Enter values for the parameters.
5. Click Save.
6. On the Admin tab menu, click Deploy Changes.

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:

Name
The text that is displayed in the right-click menu.

Description
The description of the entry. The description text is displayed in the tooltip for your menu option. The description is optional.

URL
Specifies the web address that opens in a new window. You can use the placeholder %IP%, to represent the IP address. To pass other URL parameters to this URL, you must use the `&amp;` option, for example, `url="/lookup?&amp;ip=%IP%;force=true"`.

Command
A command that you want to run on the Console. The output of the command is displayed in a new window. Use the placeholder, %IP%, to represent the IP address that is selected.

Required Capabilities
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 and flow columns

You can add more actions to the right-click options that are available on the columns in the Log Activity table or the Network 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 or flow to the URL or script.

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

1 Using SSH, log in to the 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 32: Description of the `arielRightClick.properties` file parameters

Parameter	Requirement	Description	Example
`pluginActions`	Required	Indicates either a URL or script action.	
`arielProperty`	Required	Specifies the column, or Ariel field name, for which the right-click menu is enabled.	sourceIP sourcePort destinationIP qid
`text`	Required	Specifies the text that is displayed on the right click menu.	Google search
`useFormattedValue`	Optional	Specifies whether formatted values are passed to the script. Set to **`true`** to ensure that the formatted value for attributes, such as `username` and `payload`, 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.
`url`	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: *`$Ariel_Field Name$`*	`sourceIPwebUrlAction.url= http:// www.mywebsite.com? q=$sourceIP$`
`command`	Required if the action is a command	Specifies the absolute path of the command or script file.	`destinationPortScriptAction.command=/bin/echo`
`arguments`	Required if the action is a command	Specifies the data to pass to the script. Use the following format: *`$Ariel_Field Name$`*	`destinationPortScriptAction.arguments=$qid$`

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 Extreme Security 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=$qid$-$sourcePort$-$device$-$CONTEXT$
```

Custom offense close reasons

You can manage the options listed in the Reason for Closing list box on the Offenses tab.

When a user closes an offense on the Offenses tab, the Close Offense window is displayed. The user is prompted to select a reason from the Reason for Closing list box. Three default options are listed:

- False-positive, tuned
- Non-issue
- Policy violation

Administrators can add, edit, and delete custom offense close reasons from the Admin tab.

Adding a custom offense close reason

When you add a custom offense close reason, the new reason is listed on the Custom Close Reasons window and in the Reason for Closing list box on the Close Offense window of the Offenses tab.

The Custom Offense Close Reasons window provides the following parameters.

Table 33: Custom Close Reasons window parameters

Parameter	Description
Reason	The reason that is displayed in the Reason for Closing list box on the Close Offense window of the Offenses tab.
Created by	The user that created this custom offense close reason.
Date Created	The date and time of when the user created this custom offense close reason.

1. Click the Admin tab.
2. On the navigation menu, click System Configuration.
3. Click the Custom Offense Close Reasons icon.
4. Click Add.
5. Type a unique reason for closing offenses. Reasons must be between 5 and 60 characters in length.
6. Click OK.

   Your new custom offense close reason is now listed in the Custom Close Reasons window. The Reason for Closing list box on the Close Offense window of the Offenses tab also displays the custom reason you added.

Editing custom offense close reason

Editing a custom offense close reason updates the reason in the Custom Close Reasons window and the Reason for Closing list box on the Close Offense window of the Offenses tab.

1. Click the Admin tab.
2. On the navigation menu, click System Configuration.
3. Click the Custom Offense Close Reasons icon.
4. Select the reason you want to edit.
5. Click Edit.
6. Type a new unique reason for closing offenses. Reasons must be between 5 and 60 characters in length.
7. Click OK.

Deleting a custom offense close reason

Deleting a custom offense close reason removes the reason from the Custom Close Reasons window and the *Reason for Closing* list box on the Close Offense window of the Offenses tab.

1. Click the Admin tab.
2. On the navigation menu, click System Configuration.
3. Click the Custom Offense Close Reasons icon.

4 Select the reason you want to delete.
5 Click Delete.
6 Click OK.

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 and flow properties.

Indexing event and flow 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 and flow properties that can be indexed and provides statistics for the properties. Toolbar options allow you to enable and disable indexing on selected event and flow 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 and flow properties, indexed property names are appended with the following text: *[Indexed]*. Examples of such lists include the search parameters on the *Log Activity* and *Network Activity* tab search criteria pages and the Add Filter window.

Enabling payload indexing to optimize search times

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

Restriction

Use the **Quick Filter** feature in the **Log Activity** and **Network Activity** tabs to search event and flow 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 and flow processors are at less than 70% disk usage.
- The event and flow processors are less than 70% of the maximum events per second (EPS) or flows per interface (FPI) 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 for events and flows.
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 flows or 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 or flow 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 101.

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 sets management

Using the Reference Set Management window, you can create and manage reference sets. You can also import elements into a reference set from an external file.

A reference set is a set of elements that are derived from events and flows that occur on your network. Examples of elements that are derived from events are IP addresses or user names.

After you create a reference set, you can create rules to detect log activity or network 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 or network 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 *Users Guide* for your product.

Adding a reference set

From the Admin tab, you can add a reference set that you can include in rule tests.

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

1 On the Reference Set Management window, click New.
2 Configure the parameters:

Table 34: Reference Set parameters

Parameter	Description
Name	A unique name for this reference set.
Type	You cannot edit the Type parameter after you create a reference set.
Time to Live of Elements	The amount of time that you want to maintain each element in the reference set. If you specify an amount of time, you must also indicate when you want to start tracking time for an element.

3 Click Create.

Editing a reference set

Use the Reference Set Management window to edit a reference set.

1 In the Reference Set Management window, select a reference set

2 Click Edit.

3 Edit the parameters.

Table 35: Reference Set parameters

Parameter	Description
Name	A unique name for this reference set. The maximum length is 255 characters
Type	You cannot edit the Type parameter after you create a reference set.
Time to Live of Elements	The amount of time that you want to maintain each element in the reference set. If you specify an amount of time, you must also indicate when you want to start tracking time for an element. Lives Forever is the default setting.

4 Click Submit.

Deleting reference sets

You can delete a reference set from the Reference Set Management window.

When you delete reference sets, a confirmation window indicates whether the reference sets that you want to delete have rules that are associated with them. After you delete a reference set, the Add to Reference Set configuration is cleared from the associated rules.

Tip
Before you delete a reference set, you can view associated rules in the Reference tab.

Choose one of the following options:

- On the Reference Set Management window, select a reference set, and then click Delete.
- On the Reference Set Management window, use the Quick Search text box to display only the reference sets that you want to delete, and then click Delete Listed.

Viewing the contents of a reference set

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

1 On the Reference Set Management window, select a reference set.

2 Click View Contents.

3 To view contents, click the Content tab.

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 36: Content tab parameters

Parameter	Description
Value	The value of the element. For example, if the reference contains a list of IP addresses, the value is the IP address.
Origin	The ***rulename*** is placed in the reference set as a response to a rule. The User is imported from an external file or manually added to the reference set.
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.

4 Click the References tab and view the references.

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 37: Content 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 Custom Rule or Anomaly Detection Rule.
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	System indicates a default rule. Modified indicates that a default rule was customized. User indicates a user-created rule.

5 To view or edit an associated rule, double-click the rule in the References list.

In the Rule wizard, you can edit the rule configuration settings.

Adding an element to a reference set

You add an element to a reference set by using the Reference Set Management window.

1. On the Reference Set Management window, select a reference set.
2. Click View Contents.
3. Click the Content tab.
4. On the toolbar, click New.
5. Configure the following parameters:

Parameter	Description
Value(s)	If you want to type multiple values, include a separator character between each value, and then specify the separator character in the Separator Character field.
Separator Character	Type the separator character that you used in the Value(s) field.

6. Click Add.

Deleting elements from a reference set

You can delete elements from a reference set.

1. On the Reference Set Management window, select a reference set.
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 a reference set

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.

1. On the Reference Set Management window, select a reference set.
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.

Exporting elements from a reference set

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

1. On the Reference Set Management window, select a reference set.
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**.

8 Reference data collections

Use the `ReferenceDataUtil.sh` utility to make complex reference data collections. Use reference data collections to store, retrieve, and test complex data structures.

You can create the following reference data collection types:

Reference map
: Data is stored in records that map a key to a value. For example, to correlate user activity on your network, you can create a reference map that uses the `Username` parameter as a key and the user's `Global ID` as a value.

Reference map of sets
: Data is stored in records that map a key to multiple values. For example, to test for authorized access to a patent, use a custom event property for `Patent ID` as the key and the `Username` parameter as the value. Use a map of sets to populate a list of authorized users.

Reference map of maps
: Data is stored in records that map one key to another key, which is then mapped to single value. For example, to test for network bandwidth violations, you can create a map of maps. Use the `Source IP` parameter as the first key, the `Application` parameter as the second key, and the `Total Bytes` parameter as the value.

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.

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
```

Example 3: Reference table

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

Creating a reference data collection

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.

9 Managing authorized services

You can configure authorized services on the Admin tab to authenticate a customer support service or API call for your Extreme Security deployment.

Authenticating a customer support service allows the service to connect to your Extreme Security user interface and either dismiss or update notes to an offense using a web service. You can add or revoke an authorized service at any time.

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 Analytics API Guide*.

The Manage Authorized Services window provides the following information:

Table 38: 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 SIEM.

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.

Customer support authenticated service

After you configure an authorized service, you must configure your customer support service to access Extreme Security offense information.

For example, you can configure Extreme Security to send an SNMP trap that includes the offense ID information.

Your service uses an authorized token to authenticate to Extreme Security by passing the information through an HTTP query string. When authenticated, the service interprets the authentication token as the user name during the session.

Your customer support service must use a query string to update notes, dismiss, or close an offense.

Dismiss an offense

Your customer support service must use a query string to dismiss an offense.

To dismiss an offense, your customer support service must use the following query string:

```
https://<IP address >/console/do/sem/properties?appName=Sem&
dispatch=updateProperties&id=<Offense ID>&nextPageId=
OffenseList&nextForward=offensesearch&attribute=dismiss&daoName
=offense&value=1&authenticationToken=<Token>
```

Table 39: Query string parameters for the customer support service

Parameter	Description
<IP address>	The IP address of your Extreme Security system.
<Offense ID>	The identifier that is assigned to the Extreme Security offense. To obtain the offense ID, see the Offenses tab. For more information, see the *Extreme Networks SIEM Users Guide*.
<Token>	The token identifier that is provided to the authorized service on the Extreme Security user interface.

Close an offense

Your customer support service must use a query string to close an offense.

To close an offense, your customer support service must use the following query string:

```
https://<IP Address>/console/do/sem/properties?appName=Sem&
dispatch=updateProperties&id=<Offense ID>&nextPageId=
OffenseList&nextForward=offensesearch&attribute=dismiss&daoName
=offense&value=2&authenticationToken=<Token>
```

Table 40: Query string parameters for the customer support service

Parameter	Description
<IP address>	The IP address of your Extreme Security system.
<Offense ID>	The identifier that is assigned to the Extreme Security offense. To obtain the offense ID, see the Offenses tab. For more information, see the *Extreme Networks SIEM Users Guide*.
<Token>	The token identifier that is provided to the authorized service on the Extreme Security user interface.

Add notes to an offense

You must use a query string to add notes to an offense.

To add notes to an offense, your customer support service must use the following query string:

```
https://<IP Address>/console/do/sem/properties?appName=Sem&amp;
dispatch=updateProperties&amp;id=<Offense ID>&amp;nextPageId=
OffenseList&amp;nextForward=offensesearch&amp;attribute=notes&amp;daoName
=offense&amp;value=<NOTES>&amp;authenticationToken=<Token>
```

Table 41: Query string parameters for the customer support service

Parameter	Description
<IP address>	The IP address of your Extreme Security system.
<Offense ID>	The identifier that is assigned to the Extreme Security offense. To obtain the offense ID, see the Offenses tab. For more information, see the *Extreme Networks SIEM Users Guide*.
<Token>	The token identifier that is provided to the authorized service on the Extreme Security user interface.

10 Manage backup and recovery

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 and flow data; however, you must restore event and flow data manually. For assistance in restoring your event and flow 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
- Flow sources
- Flow and event searches
- Groups
- Index management information
- License key information
- Log sources
- Offenses
- 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
- Flow 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 42: Backup Recovery Configuration parameters

Parameter	Description
General Backup Configuration	
Backup Repository Path	Type the location where you want to store your backup file. The default location is `/store/backup`. This path must exist before the backup process is initiated. If this path does not exist, the backup process aborts. If you modify this path, make sure the new path is valid on every system in your deployment. • Active data is stored on the `/store` 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 *Extreme Networks Security Offboard Storage Guide*.
Backup Retention Period (days)	Type or select the length of time, in days, that you want to store backup files. The default is 2 days. 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.
Nightly Backup Schedule	Select a backup option.

Table 42: Backup Recovery Configuration parameters (continued)

Parameter	Description
Select the managed hosts you would like to run data backups:	This option is only displayed if you select the Configuration and Data Backups option. 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. Select the check box for the managed hosts you want to run data backups on. For each host (Console or managed hosts), you can optionally clear the data items you want to exclude from the backup archive.
Configuration Only Backup	
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.
Data Backup	
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 117.

Backup archive restoration

Restoring a backup archive is useful if you want to restore previously archived configuration files, asset data, and offense 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, asset data, and offense data. For assistance in restoring your event or flow 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 43: 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 config.
Select All Configuration Items	When selected, this option indicates that all configuration items are included in the restoration of the backup archive.
Restore Configuration	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 Select All Configuration Items check box.
Select All Data Items	When selected, this option indicates that all data items are included in the restoration of the backup archive.
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. 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 44: 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 45: 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 config.
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 Select All Configuration Items 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 and flows 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 about all offenses, including source and destination IP address information, asset data, event category information, vulnerability data, event data, and flow 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.

> Restriction
> 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 SIEM 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 /`**

   > Important
   > 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 46: Description of file name variables

File name variable	Description
`hostname_hostID`	The name of the Extreme Security system that hosts the backup file followed by the identifier for the Extreme Security system
`target date`	The date that the backup file was created. The format of the target date is <*`day`*>_<*`month`*>_<*`year`*>
`backup type`	The options are **`data`** or **`config`**
`timestamp`	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 or flow 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/flows/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 or Network 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.

11 Deployment editor

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 (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 s 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 flows, 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:

- QFlow Collector 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

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 that 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, Flow Processors, 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 (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 and flows stops until the deployment completes.

Related Links

Deploying managed hosts and components after installation on page 48

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 Extreme Security QFlow Collectors, Event Processors, Extreme Security Event Collectors, off-site sources, off-site targets, and Magistrate components.

QFlow Collector

VFlow Collector collects network flows from devices on your network. Live and recorded feeds are included, such as network taps, span ports, NetFlow, and Extreme Security flow logs.

QFlow Collector groups related individual packets into a flow. A flow starts when QFlow Collector detects the first packet that has a unique source IP address, destination IP address, source port, destination port, and other specific protocol options.

Each new packet is evaluated. Counts of bytes and packets are added to the statistical counters in the flow record. At the end of an interval, a status record of the flow is sent to an Event Collector and statistical counters for the flow are reset. A flow ends when no activity for the flow is detected within the configured time.

If the protocol does not support port-based connections, Extreme Security combines all packets between the two hosts into a single flow record. However, QFlow Collector does not record flows until a connection is made to another Extreme Security component and data is retrieved.

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 flow and 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 and flows from associated Event and Flow processors.

The Data Node stores this security data to disk.

The Data Node is always connected to Event Processor or Flow 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 or flow 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 or flows 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 or flow.

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
- QFlow Collector
- 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.

   Restriction
   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 47: Description of supported component connections

Source connection	Target connection	Description
QFlow Collector	Event Collector	A QFlow Collector can connect only to an Event Collector. A QFlow Collector cannot be connected to an Event Collector of a 15xx appliance. The number of connections is not restricted.
Event Collector	Event Processor	An Event Collector can be connected only to one Event Processor. A Console Event Collector can be connected only to a Console Event Processor. This connection cannot be removed. A non-Console Event Collector can be connected to an Event Processor on the same system. A non-Console Event Collector can be connected to a remote Event Processor, but only if the Event Processor does not exist on the Console.
Event Collector	Off-site target	The number of connections is not restricted.
Off-site source	Event Collector	The number of connections is not restricted. An Event Collector connected to an Event-only appliance cannot receive an off-site connection from system hardware that has the Receive Flows feature enabled. An Event Collector connected to a QFlow-only appliance cannot receive an off-site connection from a remote system if the system has the Receive Events feature enabled.
Event Processor	Magistrate (MPC)	Only one Event Processor can connect to a Magistrate.
Event Processor	Event Processor	A Console Event Processor cannot connect to a non-Console Event Processor. A non-Console Event Processor can be connected to another Console or non-Console Event Processor, but not both at the same time. A non-Console Event Processor is connected to a Console Event Processor when a non-Console managed host is added.
Data Node	Event Processor	You can only connect a Data Node to an Event or Flow Processor. You can connect multiple Data Nodes 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. Configure flow filtering on a connection between a QFlow Collector and an Event Collector.
    a. Right-click the arrow between the QFlow Collector and the Event Collector and click **Configure**
    b. In the field for the **Flow Filter** parameter, type the IP addresses or CIDR addresses for the Extreme Security Event Collectors you want the QFlow Collector to send flows to.
5. Click **Save**.
6. Repeat these steps for all remaining components that require connections.

Forwarding normalized events and flows

To forward normalized events and flows, configure an off-site Event Collector in your current deployment to receive events and flows 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 and flow data.

    Restriction
    The off-site source must be configured with appropriate permissions to send event and flow data to the off-site target.

- An **Off-site Target** is an off-site Event Collector to which you want to send event and flow data.

Example

To forward normalized events and flows between two deployments (A and B), where deployment B wants to receive events and flows 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 -1 -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 and flows 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.

The following diagram shows forwarding event and flow between deployments.

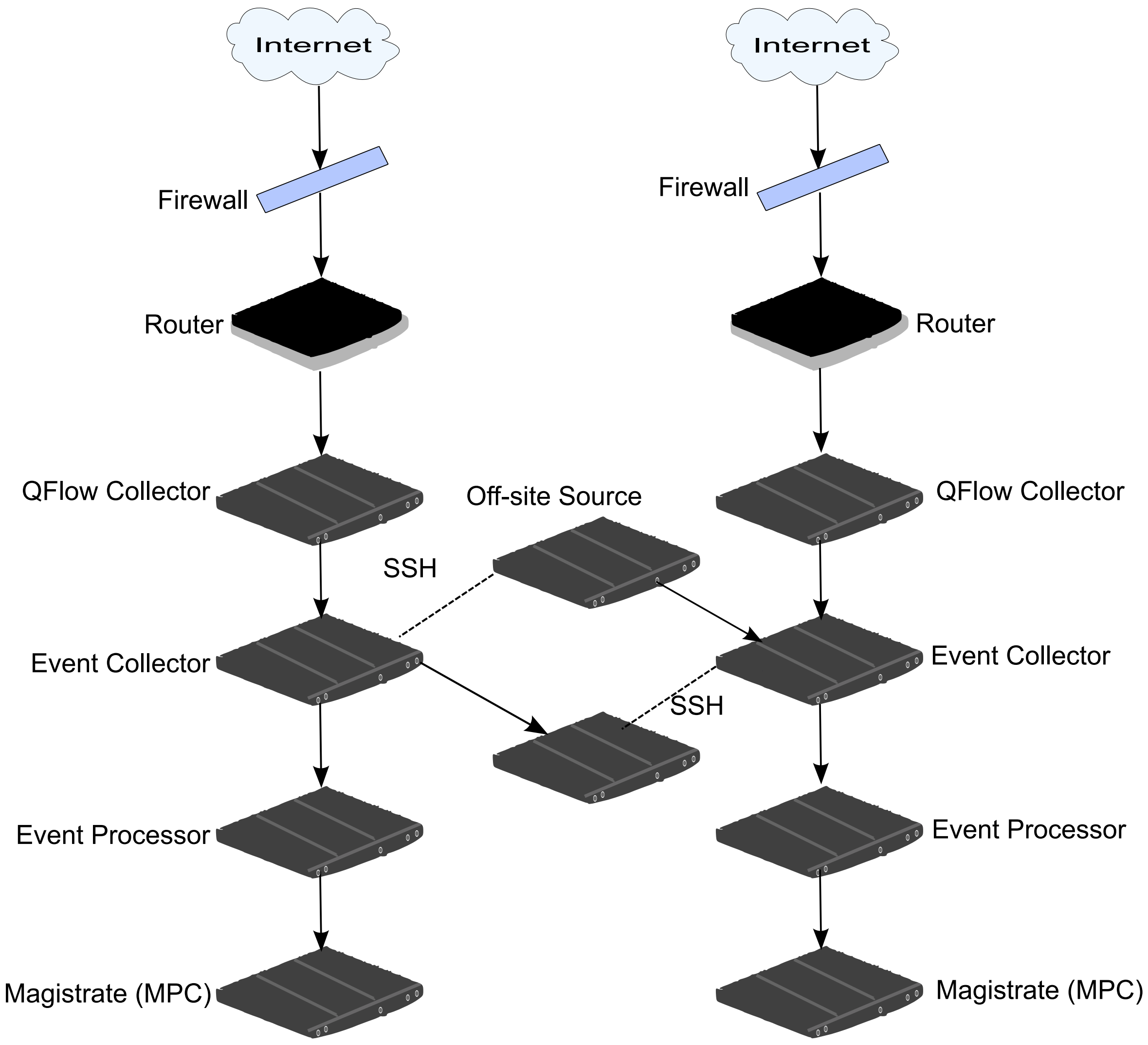

Figure 1: Forwarding events between deployments by using SSH

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 and flows 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 In Extreme SIEM, 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. When you enable encryption on the Extreme Security Console, an encryption tunnel is used when your search events by using the Offenses tab.

Tip
You can right-click a component to enable encryption between components.

Important
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 144.

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 145.

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 48: Parameters for the managed host

Header	Header
Host is NATed	Select the check box to use an existing Network Address Translation (NAT) on this managed host.
Enable Encryption	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.

4. If you selected the Host is NATed check box, configure the parameters.

Table 49: Parameters for a NAT-enabled network

Parameter	Description
Enter public IP of the server or appliance to add	The managed host uses this IP address to communicate with other managed hosts in different networks by using NAT.
Select NATed network	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.

5 Click **Next**.

6 Click **Finish**.

7 Deploy your changes.

Related Links

NAT management on page 144

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 144.

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 145.

1 Click the **System View** tab.

2 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.

3 Click **Next**.

4 Edit the parameter values, as necessary.

Use the following table to help you configure the parameters.

Table 50: Parameters for the managed host

Header	Header
Host is NATed	Select the check box to use an existing Network Address Translation (NAT) on this managed host.
Enable Encryption	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.

5 If you selected the **Host is NATed** check box, configure the parameters.

Table 51: Parameters for a NAT-enabled network

Parameter	Description
Enter public IP of the server or appliance to add	The managed host uses this IP address to communicate with other managed hosts in different networks by using NAT.
Select NATed network	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.

6. Click **Next**.
7. 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.

1. Click the **System View** tab.
2. Right-click the managed host that you want to delete and select **Remove host**.
3. Click **OK**.
4. 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 and flows stops until the deployment completes.

Configuring a managed host

Use the **System View** page of the deployment editor to configure a managed host.

1. From the **System View** page, right-click the managed host that you want to configure and click **Configure**.
2. Enter values for the parameters:

   In the **Ports to exclude** field, use a comma to separate multiple ports
3. 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 52: Host Context parameters

Parameter	Description
Warning Threshold	When the configured threshold of disk usage is exceeded, an email is sent to the administrator that indicates the current state of disk usage. 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. 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: • `/` • `/store` • `/store/tmp` Note Notification emails are sent from the email address that is specified in the Alert Email From Address parameter to the email address specified in the Administrative Email Address parameter. These parameters are configured on the System Settings window. For more information, see Set up Extreme Security on page 63.
Recovery Threshold	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%. Note Notification emails are sent from the email address that is specified in the Alert Email From Address parameter to the email address specified in the Administrative Email Address parameter. These parameters are configured on the System Settings window. For more information, see Set up Extreme Security on page 63.
Shutdown Threshold	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. Note Notification emails are sent from the email address that is specified in the Alert Email From Address parameter to the email address specified in the Administrative Email Address parameter. These parameters are configured on the System Settings window. Note For more information, see Set up Extreme Security on page 63.
Inspection Interval	The frequency, in milliseconds, that you want to determine disk usage.
Inspection Interval	The frequency, in milliseconds, that you want to inspect SAR output.

Table 52: 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 and flows 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 53: 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: `<Console>:<port>` For a non-central accumulator, type the address and port using the following syntax: `<non-Console IP Address>:<port>`
Streamer Accumulator Listen Port	The listen port responsible for receiving streams of flows from the Event Processor. The default value is 7802.
Alerts DSM Address	The device system module (DSM) address that is used to forwarding alerts from the accumulator. Use the following syntax: `<DSM_IP address>:<DSM port number>` .

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.

> **Important**
> 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 54: 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 NAT management on page 144.

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 and flows stops until the deployment completes.

Component configuration

Use the deployment editor to configure each component in your deployment.

Configuring a QFlow Collector

Use the deployment editor to configure a QFlow Collector.

You can configure a flow filter on the connection from a QFlow Collector and multiple Extreme Security Event Collectors. A flow filter controls which flow a component receives. The Flow Filter parameter is available on the Flow Connection Configuration window.

Right-click the arrow between the component you want to configure for flow filtering and select Configure.

The following table describes the advanced QFlow Collector parameters:

1. From either the Event View or System View page, select the QFlow Collector you want to configure.
2. Click Actions > Configure.
3. Enter values for the following parameters:

Parameter	Description
Event Collector Connections	The Event Collector component that is connected to this QFlow Collector. The connection is displayed in the following format: `<Host IP Address>:<Port>.` If the QFlow Collector is not connected to an Event Collector, the parameter is empty.
QFlow CollectorID	A unique ID for the QFlow Collector.
Maximum Content Capture	The capture length, in bytes, to attach to a flow. The range is 0 - 65535. A value of 0 disables content capture. The default is 64 bytes. Extreme Security QFlow Collectors capture a configurable number of bytes at the start of each flow. Transferring large amounts of content across the network might affect network and performance. On managed hosts where the Extreme Security QFlow Collectors are on close high-speed links, you can increase the content capture length. Important Increasing content capture length increases disk storage requirements for suggested disk allotment.
Alias Autodetection	The Yes option enables the QFlow Collector to detect external flow source aliases. When a QFlow Collector receives traffic from a device with an IP address, but no current alias, the QFlow Collector attempts a reverse DNS lookup to determine the host name of the device. If the lookup is successful, the QFlow Collector adds this information to the database and reports this information to all your deployment. The No option prevents the QFlow Collector from detecting external flow sources aliases.

4. On the toolbar, click Advanced to display the advanced parameters.

5 Enter values for the advanced parameters, as necessary.

Table 55: Advanced QFlow Collector parameters:

Parameter	Description
Event Collector Connections	The Event Collector connected to this QFlow Collector. The connection is displayed in the following format: `<Host IP Address>:<Port>`. If the QFlow Collector is not connected to an Event Collector, the parameter is empty.
Flow Routing Mode	The 0option enables **Distributor Mode**, which allows QFlow Collector to group flows that have similar properties. The 1 option enables **Flow Mode**, which prevents the bundling of flows
Maximum Data Capture/Packet	The number of bytes and packets that you want the QFlow Collector to capture.
Time Synchronization Server IP Address	The IP address or host name of the time server.
Time Synchronization Timeout Period	The length of time that you want the managed host to continue attempting to synchronize the time before timing out. The default is 15 minutes.
Endace DAG Interface Card Configuration	The Endace network monitoring interface card parameters. For more information about the required input for this parameter, contact Customer Support (www.extremenetworks.com/support/).
Flow Buffer Size	The amount of memory, in MB, that you want to reserve for flow storage. The default is 400 MB.
Maximum Number of Flows	The maximum number of flows you want to send from the QFlow Collector to an Event Collector.
Remove duplicate flows	The **Yes** option enables the QFlow Collector to remove duplicate flows. The **No** option prevents the QFlow Collector from removing duplicate flows.
Verify NetFlow Sequence Numbers	The **Yes** enables the QFlow Collector to check the incoming NetFlow sequence numbers to ensure that all packets are present and in order. A notification is displayed if a packet is missing or received out-of-order.
External Flow De-duplication method	The method that you want to use to remove duplicate external flow sources (de-duplication): • The **Source** enables the QFlow Collector to compare originating flow sources. This method compares the IP address of the device that exported the current external flow record to that of the IP address of the device that exported the first external record of the particular flow. If the IP addresses do not match, the current external flow record is discarded. • The **Record** option enables the QFlow Collector to compare individual external flow records. This method logs a list of every external flow record that is detected by a particular device and compares each subsequent record to that list. If the current record is found in the list, that record is discarded.
Flow Carry-over Window	The number of seconds before the end of an interval that you want one-sided flows to be held over until the next interval if the flow. This setting allows time for the inverse side of the flow to arrive before it is reported.

Table 55: Advanced QFlow Collector parameters: (continued)

Parameter	Description
External flow record comparison mask	• This parameter is only valid if you typed Record in the External Flow De-duplication method parameter. The external flow record fields that you want to use to remove duplicate flows include the following options: • D (direction) • B (ByteCount) • P (PacketCount) You can combine these options. Possible combinations of the options include the following combinations: • The DBP option uses direction, byte count, and packet count when it compares flow records. • The XBP option uses byte count and packet count when it compares flow records. • The DXP option uses direction and packet count when it compares flow records. • The DBX option uses direction and byte count when it compares flow records. • The DXX option uses direction when it compares flow records. • The XBX option uses byte count when it compares records. • The XXP option uses packet count when it compares records.
Create Superflows	The Yes option enables the QFlow Collector to create superflows from group flows that have similar properties. The No option prevents the creation of superflows.
Type A Superflows	The threshold for type A superflows. A type A superflow is a group of flows from one host to many hosts. This flow is a unidirectional flow that is an aggregate of all flows that have different destination hosts, but the following parameters are the same: • Protocol • Source bytes • Source hosts • Destination network • Destination port (TCP and UDP flows only) • TCP flags (TCP flows only) • ICMP type, and code (ICMP flows only)
Type B Superflows	The threshold for type B superflows. A type B superflow is group of flows from many hosts to one host. This flow is unidirectional flow that is an aggregate of all flows that have different source hosts, but the following parameters are the same: • Protocol • Source bytes • Source packets • Destination host • Source network • Destination port (TCP and UDP flows only) • TCP flags (TCP flows only) • ICMP type, and code (ICMP flows only)

Table 55: Advanced QFlow Collector parameters: (continued)

Parameter	Description
Type C Superflows	The threshold for type C superflows. Type C superflows are a group of flows from one host to another host. This flow is a unidirectional flow that is an aggregate of all non-ICMP flows have different source or destination ports, but the following parameters are the same: • Protocol • Source host • Destination host • Source bytes • Destination bytes • Source packets • Destination packets
Recombine Asymmetric Superflows	In some networks, traffic is configured to take alternate paths for inbound and outbound traffic. This routing is called asymmetric routing. You can combine flows that are received from one or more QFlow Collector. However, if you want to combine flows from multiple QFlow Collector components, you must configure flow sources in the Asymmetric Flow Source Interface(s) parameter in the QFlow Collector configuration. • The Yes option enables the QFlow Collector to recombine asymmetric flows. • The No option prevents the QFlow Collector from recombining asymmetric flows.
Ignore Asymmetric Superflows	The Yes option enables the QFlow Collector to create superflows while asymmetric flows are enabled. The No option prevents the QFlow Collector from creating superflows while asymmetric flows are enabled.
Minimum Buffer Data	The minimum amount of data, in bytes, that you want the Endace network monitoring interface card to receive before the captured data is returned to the QFlow Collector process. If this parameter is 0 and no data is available, the Endace network monitoring interface card allows non-blocking behavior.
Maximum Wait Time	The maximum amount of time, in microseconds, that you want the Endace network monitoring interface card to wait for the minimum amount of data. The minimum amount of data is specified in the Minimum Buffer Data parameter.
Polling Interval	The interval, in microseconds, that you want the Endace network monitoring interface card to wait before it checks for more data. A polling interval avoids excessive polling traffic to the card and, therefore, conserves bandwidth and processing time.

6 Click Save.

7 Repeat for all Extreme Security QFlow Collectors in your deployment you want to configure.

Related Links

Event views of Extreme Security components in your deployment on page 129

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
Destination Event Processor	Specifies the Event Processor component that is connected to this Event Collector. The connection is displayed in the following format: `<Host IP Address>:<Port>`.
Flow Listen Port	The listen port for flows.
Event Forwarding Listen Port	The Event Collector event forwarding port.
Flow Forwarding Listen Port	The Event Collector flow forwarding port.

4 On the toolbar, click Advanced to display the advanced parameters.

5 Configure the advanced parameters, as necessary.

Table 56: Event Collector advanced parameters

Parameter	Description
Primary Collector	True specifies that the Event Collector is on a Console system. False specifies that the Event Collector is on a non-Console system.
Autodetection Enabled	Yes 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. No prevents the Event Collector from automatically analyzing and accepting traffic from previously unknown log sources. For more information, see the *Extreme Networks Security Managing Log Sources Guide*.
Flow Deduplication Filter	The amount of time in seconds that flows are buffered before they are forwarded.
Asymmetric Flow Filter	The amount of time in seconds that asymmetric flow is buffered before they are forwarded.
Forward Events Already Seen	True enables the Event Collector to forward events that was detected on the system. False 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 129

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 57: 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 58: Event Processor advanced parameters

Parameter	Description
Test Rules	The test rules list is available only for non-Console Event Processors. If a rule is configured to test locally, the Globally option does not override the rule setting. If you select Locally, rules are tested on the Event Processor and not shared with the system. If you select Globally, individual rules for every Event Processor are shared and tested system wide. Each rule can be toggled to Global for detection by any Event Processor on the system. 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. Testing rules globally is the default for non-Csonsole Event Processor with each rule on the Event Processor set to test locally.
Overflow Event Routing Threshold	Type the events per second threshold that Event Processor can manage. Events over this threshold are placed in the cache.
Overflow Flow Routing Threshold	Type the flows per minute threshold that the Event Processor can manage. Flows over this threshold are placed in the cache.
Events database path	Type the location that you want to store events. The default is /store/ariel/events.
Payloads database length	The location that you want to store payload information. The default is /store/ariel/payloads.

6 Click Save.

7 Repeat for all Event Processor in your deployment you want to configure.

Related Links

Event views of Extreme Security components in your deployment on page 129

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 129

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
Receive Events	**True** enables the system to receive events from the off-site source host. **False** prevents the system from receiving events from the off-site source host.
Receive Flows	**True** enables the system to receive flows from the off-site source host. **False** prevents the system from receiving flows 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 129

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.
Flow Collector Listen Port	The Event Collector listening port for receiving flow data. The default port for flows is 32000.

4 Click **Save**.

Related Links

Event views of Extreme Security components in your deployment on page 129

12 Flow sources management

Use the Flow Sources window to manage the flow sources in your deployment.

You can add, edit, enable, disable, or delete flow sources.

Related Links

Flow sources management on page 154
Use the Flow Sources window to manage the flow sources in your deployment.

Flow sources

For Extreme Networks Security Analytics appliances, Extreme SIEM automatically adds default flow sources for the physical ports on the appliance. Extreme SIEM also includes a default NetFlow flow source.

If Extreme SIEM is installed on your own hardware, Extreme SIEM attempts to automatically detect and add default flow sources for any physical devices, such as a network interface card (NIC). Also, when you assign a QFlow Collector, Extreme SIEM includes a default NetFlow flow source.

With Extreme SIEM you can integrate flow sources.

Flow sources are classed as either internal or external:

Internal flow sources

Includes any additional hardware that is installed on a managed host, such as a network interface card (NIC). Depending on the hardware configuration of your managed host, the internal flow sources might include the following sources:

- Network interface card
- Endace network monitoring interface card
- Napatech interface

External flow sources

Includes any external flow sources that send flows to the QFlow Collector. If your QFlow Collector receives multiple flow sources, you can assign each flow source a distinct name. When external flow data is received by the same QFlow Collector, a distinct name helps to distinguish external flow source data from each other.

External flow sources might include the following sources:

- NetFlow
- IPFIX

- sFlow
- J-Flow
- PacketeerPacketeer
- Flowlog file

Extreme SIEM can forward external flows source data by using the spoofing or non-spoofing method:

Spoofing
: Resends the inbound data that is received from flow sources to a secondary destination. To ensure that flow source data is sent to a secondary destination, configure the Monitoring Interface parameter in the flow source configuration to the port on which data is received (management port). When you use a specific interface, the QFlow Collector uses a promiscuous mode capture to obtain flow source data, rather than the default UDP listening port on port 2055. As a result, QFlow Collector can capture flow source packets and forward the data.

Non-Spoofing
: For the non-spoofing method, configure the Monitoring Interface parameter in the flow source configuration as **Any**. The QFlow Collector opens the listening port, which is the port that is configured as the Monitoring Port to accept flow source data. The data is processed and forwarded to another flow source destination. The source IP address of the flow source data becomes the IP address of the Extreme SIEM system, not the original router that sent the data.

NetFlow

NetFlow is a proprietary accounting technology that is developed by Cisco Systems. NetFlow monitors traffic flows through a switch or router, interprets the client, server, protocol, and port that is used, counts the number of bytes and packets, and sends that data to a NetFlow collector.

The process of sending data from NetFlow is often referred to as a NetFlow Data Export (NDE). You can configure Extreme SIEM to accept NDEs and thus become a NetFlow collector. Extreme SIEM supports NetFlow versions 1, 5, 7, and 9. For more information on NetFlow, see the Cisco web site (http://www.cisco.com).

While NetFlow expands the amount of the network that is monitored, NetFlow uses a connection-less protocol (UDP) to deliver NDEs. After an NDE is sent from a switch or router, the NetFlow record is purged. As UDP is used to send this information and does not guarantee the delivery of data, NetFlow records inaccurate recording and reduced alerting capabilities. Inaccurate presentations of both traffic volumes and bidirectional flows might result.

When you configure an external flow source for NetFlow, you must do the following tasks:

- Make sure that the appropriate firewall rules are configured. If you change your External Flow Source Monitoring Port parameter in the QFlow Collector configuration, you must also update your firewall access configuration.
- Make sure that the appropriate ports are configured for your QFlow Collector.

If you are using NetFlow version 9, make sure that the NetFlow template from the NetFlow source includes the following fields:

- FIRST_SWITCHED
- LAST_SWITCHED
- PROTOCOL
- IPV4_SRC_ADDR
- IPV4_DST_ADDR

- L4_SRC_PORT
- L4_DST_PORT
- IN_BYTES or OUT_BYTES
- IN_PKTS or OUT_PKTS
- TCP_FLAGS (TCP flows only)

Related Links

Deployment editor on page 126

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.

IPFIX

Internet Protocol Flow Information Export (IPFIX) is an accounting technology. IPFIX monitors traffic flows through a switch or router, interprets the client, server, protocol, and port that is used, counts the number of bytes and packets, and sends that data to a IPFIX collector.

IBM® Security Network Protection XGS 5000, a next generation intrusion protection system (IPS), is an example of a device that sends flow traffic in IPFIX flow format.

The process of sending IPFIX data is often referred to as a NetFlow Data Export (NDE). IPFIX provides more flow information and deeper insight than NetFlow v9. You can configure Extreme SIEM to accept NDEs and thus become an IPFIX collector. IPFIX uses User Datagram Protocol (UDP) to deliver NDEs. After an NDE is sent from the IPFIX forwarding device, the IPFIX record might be purged.

To configure Extreme SIEM to accept IPFIX flow traffic, you must add a NetFlow flow source. The NetFlow flow source processes IPFIX flows by using the same process.

Your Extreme SIEM system might include a default NetFlow flow source; therefore, you might not be required to configure a NetFlow flow source. To confirm that your system includes a default NetFlow flow source, select Admin > Flow Sources. If default_Netflow is listed in the flow source list, IPFIX is already configured.

When you configure an external flow source for IPFIX, you must do the following tasks:

- Ensure that the appropriate firewall rules are configured. If you change your External Flow Source Monitoring Port parameter in the QFlow Collector configuration, you must also update your firewall access configuration. For more information about QFlow Collector configuration, see the *Extreme Networks SIEM Administration Guide*.
- Ensure that the appropriate ports are configured for your QFlow Collector.
- Ensure the IPFIX template from the IPFIX source includes the following fields:
- FIRST_SWITCHED
- LAST_SWITCHED
- PROTOCOL
- IPV4_SRC_ADDR
- IPV4_DST_ADDR
- L4_SRC_PORT
- L4_DST_PORT

- IN_BYTES or OUT_BYTES
- IN_PKTS or OUT_PKTS
- TCP_FLAGS (TCP flows only)

sFlow

sFlow is a multi-vendor and user standard for sampling technology that provides continuous monitoring of application level traffic flows on all interfaces simultaneously.

A sFlow combines interface counters and flow samples into sFlow datagrams that are sent across the network to an sFlow collector. Extreme SIEM supports sFlow versions 2, 4, and 5. sFlow traffic is based on sampled data and, therefore, might not represent all network traffic. For more information, see the sflow website (www.sflow.org).

sFlow uses a connection-less protocol (UDP). When data is sent from a switch or router, the sFlow record is purged. As UDP is used to send this information and does not guarantee the delivery of data, sFlow records inaccurate recording and reduced alerting capabilities. Inaccurate presentations of both traffic volumes and bidirectional flows might result.

When you configure an external flow source for sFlow, you must do the following tasks:

- Make sure that the appropriate firewall rules are configured.
- Make sure that the appropriate ports are configured for your VFlow Collector.

J-Flow

A proprietary accounting technology used by Juniper Networks that allows you to collect IP traffic flow statistics. J-Flow enables you to export data to a UDP port on a J-Flow collector. Using J-Flow, you can also enable J-Flow on a router or interface to collect network statistics for specific locations on your network. Note that J-Flow traffic is based on sampled data and, therefore, might not represent all network traffic. For more information on J-Flow, see the Juniper Networks website (www.juniper.net).

J-Flow uses a connection-less protocol (UDP). When data is sent from a switch or router, the J-Flow record is purged. As UDP is used to send this information and does not guarantee the delivery of data, J-Flow records inaccurate recording and reduced alerting capabilities. This can result in inaccurate presentations of both traffic volumes and bi-directional flows.

When you configure an external flow source for J-Flow, you must:

- Make sure the appropriate firewall rules are configured.
- Make sure the appropriate ports are configured for your QFlow Collector.

Packeteer

Packeteer devices collect, aggregate, and store network performance data. After you configure an external flow source for Packeteer, you can send flow information from a Packeteer device to Extreme SIEM.

Packeteer uses a connection-less protocol (UDP). When data is sent from a switch or router, the Packeteer record is purged. As UDP is used to send this information and does not guarantee the delivery of data, Packeteer records inaccurate recording and reduced alerting capabilities. Inaccurate presentations of both traffic volumes and bidirectional flows might occur.

To configure Packeteer as an external flow source, you must do the following tasks:

- Make sure that the appropriate firewall rules are configured.
- Make sure that you configure Packeteer devices to export flow detail records and configure the QFlow Collector as the destination for the data export.
- Make sure that the appropriate ports are configured for your QFlow Collector.
- Make sure the class IDs from the Packeteer devices can automatically be detected by the QFlow Collector.
- For more information, see the *Mapping Packeteer Applications into Extreme Security Technical Note*.

Flowlog file

A Flowlog file is generated from the Extreme SIEM flow logs.

Napatech interface

If you installed a Napatech Network Adapter on your Extreme SIEM system, the Napatech Interface option is displayed as a configurable packet-based flow source on the Extreme SIEM user interface. The Napatech Network Adapter provides next-generation programmable and intelligent network adapter for your network. For more information, see the Napatech documentation.

Adding or editing a flow source

Use the Flow Source window to add a flow source.

1. Click the Admin tab.
2. On the navigation menu, click Data Sources.
3. On the navigation menu, click Flows.
4. Click Flow Sources.
5. Do one of the following actions:
   - To add a flow source, click Add.
   - To edit a flow source, select the flow source and click Edit.
6. To create this flow source from an existing flow source, select the Build from existing flow source check box, and select a flow source from the Use as Template list.
7. Enter the name for the Flow Source Name.

   Tip
   If the external flow source is also a physical device, use the device name as the flow source name. If the flow source is not a physical device, use a recognizable name.

   For example, if you want to use IPFIX traffic, enter ipf1. If you want to use NetFlow traffic, enter nf1.

8. Select a flow source from the Flow Source Type list and configure the properties.
    - If you select the Flowlog File option, ensure that you configure the location of the Flowlog file for the Source File Path parameter.
    - If you select the JFlow, Netflow, Packeteer FDR, or sFlow options in the Flow Source Type parameter, ensure that you configure an available port for the Monitoring Port parameter.

      The default port for the first NetFlow flow source that is configured in your network is 2055. For each additional NetFlow flow source, the default port number increments by 1. For example, the default NetFlow flow source for the second NetFlow flow source is 2056.
    - If you select the Napatech Interface option, enter the Flow Interface that you want to assign to the flow source.

      Restriction
      The Napatech Interface option is displayed only if you installed the Napatech Network Adapter on your system.
    - If you select the Network Interface option, for the Flow Interface, configure only one log source for each Ethernet interface.

      Restriction
      You cannot send different flow types to the same port.
9. If traffic on your network is configured to take alternate paths for inbound and outbound traffic, select the Enable Asymmetric Flows check box.
10. Click Save.
11. On the Admin tab menu, click Deploy Changes.

Enabling and disabling a flow source

Using the Flow Source window, you can enable or disable a flow source.

1. Click the Admin tab.
2. On the navigation menu, click Data Sources.
3. On the navigation menu, click Flows.
4. Click the Flow Sources icon.
5. Select the flow source that you want to enable or disable.

   The Enabled column indicates whether the flow source is enabled or disabled.

   The following statuses are displayed:
    - True indicates that the flow source is enabled.
    - False indicates that the flow source is now disabled.
6. Click Enable/Disable.
7. On the Admin tab menu, click Deploy Changes.

Deleting a Flow Source

Use the Flow Source window to delete a flow source.

1. Click the **Admin** tab.
2. On the navigation menu, click **Data Sources**.
3. On the navigation menu, click **Flows**.
4. Click **Flow Sources**.
5. Select the flow source that you want to delete.
6. Click **Delete**.
7. Click **OK**.
8. On the **Admin** tab menu, click **Deploy Changes**.

Flow source aliases management

You can use the **Flow Source Alias** window to configure virtual names, or aliases, for your flow sources.

You can identify multiple sources that are sent to the same QFlow Collector by using the source IP address and virtual name. With an alias, a QFlow Collector can uniquely identify and process data sources that are sent to the same port.

When QFlow Collector receives traffic from a device that has an IP address but does not have a current alias, the QFlow Collector attempts a reverse DNS lookup. The lookup is used to determine the host name of the device. If the lookup is successful, the QFlow Collector adds this information to the database and reports the information to all QFlow Collector components in your deployment.

Use the deployment editor to configure the QFlow Collector to automatically detect flow source aliases.

Adding or a flow source alias

Use the **Flow Source Alias** window to add a flow source alias.

1. Click the **Admin** tab.
2. On the navigation menu, click **Data Sources**.
3. On the navigation menu, click **Flows**.
4. Click the **Flow Source Aliases** icon.
5. Do one of the following actions:
   - To add a flow source alias, click **Add** and enter the values for the parameters.
   - To edit an existing flow source alias, select the flow source alias, click **Edit**, and update the parameters.
6. Click **Save**.
7. On the **Admin** tab menu, click **Deploy Changes**.

Deleting a flow source alias

Use the **Flow Source Alias** window to delete a flow source alias.

1. Click the **Admin** tab.
2. On the navigation menu, click **Data Sources**.

3. On the navigation menu, click Flows.
4. Click the Flow Source Aliases icon.
5. Select the flow source alias that you want to delete.
6. Click Delete.
7. Click OK.
8. On the Admin tab menu, click Deploy Changes.

13 Remote networks and services configuration

Use remote network and service groups to represent traffic activity on your network for a specific profile. Remote networks groups display user traffic that originates from named remote networks.

All remote network and service groups have group levels and leaf object levels. You can edit remote network and service groups by adding objects to existing groups or changing pre-existing properties to suit your environment.

If you move an existing object to another group, the object name moves from the existing group to the newly selected group. However, when the configuration changes are deployed, the object data that is stored in the database is lost and the object ceases to function. To resolve this issue, create a new view and re-create the object that exists with another group.

On the Admin tab, you can group remote networks and services for use in the custom rules engine, flow, and event searches. You can also group networks and services in Extreme Networks Security Risk Manager, if it is available.

Default remote network groups

Extreme SIEM includes default remote network groups:

The following table describes the default remote network groups.

Table 59: Default remote network groups

Group	Description
BOT	Specifies traffic that originates from BOT applications.
Bogon	Specifies traffic originating from un-assigned IP addresses. For more information, see the bogon reference on the Team CYMRU web site (http://www.team-cymru.org/Services/Bogons).
HostileNets	Specifies traffic that originates from known hostile networks. HostileNets has a set of 20 (rank 1 - 20 inclusive) configurable CIDR ranges.

Table 59: Default remote network groups (continued)

Group	Description
Neighbours	This group is blank by default. You must configure this group to classify traffic that originates from neighboring networks.
Smurfs	Specifies traffic that originates from smurf attacks. A smurf attack is a type of denial-of-service attack that floods a destination system with spoofed broadcast ping messages.
Superflows	This group is non-configurable. A superflow is a flow that is an aggregate of a number of flows that have a similar predetermined set of elements.
TrustedNetworks	This group is blank by default. You must configure this group to classify traffic that originates from trusted networks.
Watchlists	This group is blank by default. You can configure this group to classify traffic that originates from networks you want monitor.

Groups and objects that include superflows are only for informational purposes and cannot be edited. Groups and objects that include bogons are configured by the Automatic Update function.

Default remote service groups

Extreme SIEM includes the default remote service groups.

The following table describes the default remote service groups.

Table 60: Default remote network groups

Parameter	Description
IRC_Servers	Specifies traffic that originates from addresses commonly known as chat servers.
Online_Services	Specifies traffic that originates from addresses commonly known online services that might involve data loss.
Porn	Specifies traffic that originates from addresses commonly known to contain explicit pornographic material.
Proxies	Specifies traffic that originates from commonly known open proxy servers.
Reserved_IP_ Ranges	Specifies traffic that originates from reserved IP address ranges.
Spam	Specifies traffic that originates from addresses commonly known to produce SPAM or unwanted email.
Spy_Adware	Specifies traffic that originates from addresses commonly known to contain spyware or adware.
Superflows	Specifies traffic that originates from addresses commonly known to produce superflows.
Warez	Specifies traffic that originates from addresses commonly known to contain pirated software.

Guidelines for network resources

Given the complexities and network resources that are required for Extreme SIEM in large structured networks, follow the suggested guidelines.

The following list describes some of the suggested practices that you can follow:

- Bundle objects and use the Network Activity and Log Activity tabs to analyze your network data.

  Fewer objects create less input and output to your disk.
- Typically, for standard system requirements, do not exceed more than 200 objects per group.

  More objects might impact your processing power when you investigate your traffic.

Managing remote networks objects

After you create remote network groups, you can aggregate flow and event search results on remote network groups. You can also create rules that test for activity on remote network groups.

Use the Remote Networks window, you can add or edit a remote networks object.

1. Click the Admin tab.
2. On the navigation menu, click Remote Networks and Services Configuration.
3. Click the Remote Networks icon.
4. To add a remote networks object, click Add and enter values for the parameters.
5. To edit remote networks object, click the group that you want displayed, click Edit, and then change the values.
6. Click Save.
7. Click Return.
8. Close the Remote Networks window.
9. On the Admin tab menu, click Deploy Changes.

Managing remote services objects

Remote services groups organize traffic that originates from user-defined network ranges or the IBM automatic update server. After you create remote service groups, you can aggregate flow and event search results, and create rules that test for activity on remote service groups.

Use the Remote Services window to add or edit a remote services object.

1. Click the Admin tab.
2. On the navigation menu, click Remote Networks and Services Configuration.
3. Click the Remote Services icon.
4. To add a remote services object, click Add and enter the parameter values.
5. To edit a remote services object, click the group that you want displayed, click the Edit icon and change the values.
6. Click Save.
7. Click Return.

8 Close the **Remote Services** window.
9 On the **Admin** tab menu, click **Deploy Changes**.

QID map overview

Use the QRadar Identifier (QID) map utility to create, export, import, or modify user-defined QID map entries.

The QID map associates an event on an external device to a (QID).

See the following tasks for QID management:

- Creating a QID map entry on page 165
- Modifying a QID map entry on page 166
- Importing Qid map entries on page 167
- Exporting QID map entries on page 169

To run the utility, use the following syntax:

```
qidmap_cli.sh [-l|-c|-m|-i[-f <filename>]|-e[-f <filename>]|-d]
```

The following table describes the command-line options for the QID map utility.

Table 61: QID map utility options

Options	Description
-l	Lists the low-level category.
-c	Creates a QID map entry
-m	Modifies an existing user-defined QID map entry.
-i	Imports QID map entries.
-e	Exports existing user-defined QID map entries.
-f <filename>	If you include the -i or -e option, specifies a file name to import or export QID map entries.
-d	If you include the -i or -e option, specifies a delimiter for the import or export file. The default is a comma.
-h	Displays the help options.

Creating a QID map entry

Create a QRadar Identifier (QID) Map Entry to map an event of an external device to QID.

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

2 To locate the low-level category for the QID map entry that you want to create, type the following command:

```
/opt/qradar/bin/qidmap_cli.sh -l
```

If you want to search for a particular low-level category, you can use the `grep` command to filter the results:

```
/opt/qradar/bin/qidmap_cli.sh -l | grep <text>
```

3 Type the following command:

```
qidmap_cli.sh -c --qname <name> --qdescription <description>
--severity <severity> --lowlevelcategoryid <ID>
```

The following table describes the command-line options for the QID map utility:

Options	Description
-c	Creates a QID map entry.
--qname <name>	The name that you want to associate with this QID map entry. The name can be up to 255 characters in length, with no spaces.
--qdescription <description>	The description for this QID map entry. The description can be up to 2048 characters in length with no spaces.
--severity <severity>	The severity level that you want to assign to this QID map entry. The valid range is 0 - 10.
--lowlevelcategoryid <ID>	The low-level category ID you want to assign to this QID map entry. For more information, see the *Extreme Networks SIEM Administration Guide*.

Modifying a QID map entry

Modify an existing user-defined QRadar Identifier (QID) map entry.

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

2 Type the following command:

```
qidmap_cli.sh -m --qid<QID> --qname <name> --qdescription <description>
--severity <severity>
```

The following table describes the command-line options for the QID map utility:

Options	Description
-m	Modifies an existing user-defined QID map entry.
--qid<QID>	The QID that you want to modify.
--qname <name>	The name that you want to associate with this QID map entry. The name can be up to 255 characters in length with no spaces.
--qdescription <description>	The description for this QID map entry. The description can be up to 2048 characters in length with no spaces.
--severity <severity>	The severity level that you want to assign to this QID map entry. The valid range is 0 - 10.

Importing Qid map entries

Using the QRadar Identifier (QID) map utility, you can import QID map entries from a .txt file.

1. Create a `.txt` file that includes the user-defined QID map entries that you want to import. Ensure that each entry in the file is separated with a comma. Choose one of the following options:
   - If you want to import a new list of user-defined QID map entries, create the file with the following format for each entry:

     ```
     ,<name>,<description>,<severity>,<category>
     ```

     Example

     ```
     ,buffer,buffer_QID,7,18401 ,malware,malware_misc,8,18403
     ```

   - If you want to import an existing list of user-defined QID map entries, create the file with the following format for each entry:

     ```
     <qid>,<name>,<description>,<severity>
     ```

     Example

     ```
     2000002,buffer,buffer_QID,7 2000001,malware,malware_misc
     ```

   The following table describes the command-line options of the QID utility.

Options	Description
<qid>	The existing QID for the entry. This option is required if you want to import an existing exported list of QID entries. To import new QID entries, do not use this option. The QID map utility assigns an identifier (QID) for each entry in the file.
--qname <name>	The name that you want to associate with this QID map entry. The name can be up to 255 characters in length with no spaces.
--qdescription <description>	The description for this QID map entry. The description can be up to 2048 characters in length with no spaces.
--severity <severity>	The severity level that you want to assign to this QID map entry. The valid range is 0 - 10.
--lowlevelcategoryid <ID>	The low-level category ID that you want to assign to this QID map entry. This option is only necessary if you want to import a new list of QID entries.

2. Save and close the file.
3. Using SSH, log in to Extreme Security as the root user:
4. To import the QID map file, type the following command:

   ```
   /opt/qradar/bin/qidmap_cli.sh -i -f <filename.txt>
   ```

   The *<filename.txt>* option is the directory path and name of the file that contains the QID map entries. If any of the entries in the file cause an error, no entries in the file are enforced.

Exporting QID map entries

Using the QRadar Identifier (QID) map utility, you can export user-defined QID map entries to a `.txt` file.

1. Using SSH, log in to Extreme Security as the root user.
2. To export the QID map file, type the following command:

   ```
   /opt/qradar/bin/qidmap_cli.sh -e -f <filename.txt>
   ```

   The ***<filename.txt>*** option is the directory path and name of the file that you want to contain your QID map entries.

14 Server discovery

Discovering servers

The Server Discovery function uses the Asset Profile database to discover different server types that are based on port definitions. Then, you can select the servers to add to a server-type building block for rules.

The Server Discovery function is based on server-type building blocks. Ports are used to define the server type. Thus, the server-type building block works as a port-based filter when you search the Asset Profile database.

For more information about building blocks, see the *Extreme Networks SIEM Users Guide*.

Discovering servers

Use the Assets tab to discover servers on your network.

1. Click the Assets tab
2. On the navigation menu, click Server Discovery.
3. From the Server Type list, select the server type that you want to discover.
4. Select one of the following options to determine the servers you want to discover:
    - To use the currently selected Server Type to search all servers in your deployment, select All.
    - To search servers in your deployment that were assigned to the currently selected Server Type, select Assigned.
    - To search servers in your deployment that are not assigned, select Unassigned.
5. From the Network list, select the network that you want to search.
6. Click Discover Servers.
7. In the Matching Servers table, select the check boxes of all servers you want to assign to the server role.
8. Click Approve Selected Servers.

15 Domain segmentation

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 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 and flows 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 and flows 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 and flow 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 Extreme Security input sources. When events and flows come into Extreme Security, the domain definitions are evaluated and the events and flows are tagged with the domain information.

Specifying domains for events

These are the ways to specify domains for events:

Event collectors

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.

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.

Log sources

You can configure specific log sources to belong to a domain.

This method of tagging domains is an option for deployments in which an event collector can receive events from multiple domains.

Log source groups

You can assign log source groups to a specific domain. This option allows broader control over the log source configuration.

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.

Custom properties

You can apply custom properties to the log messages that come from a log source.

To determine which domain that specific log messages belong to, the value of the custom property is looked up against a user-defined table.

This option is used for multi-address-range or multi-tenant log sources, such as file servers and document repositories.

Specifying domains for flows

These are the ways to specify domains for flows:

Flow collectors

You can assign specific QFlow collectors to a domain.

All flow sources that arrive at that flow collector belong to the domain; therefore, any new auto-detected flow sources are automatically added to the domain.

Flow sources

You can designate specific flow sources to a domain.

This option is useful when a single QFlow collector is collecting flows from multiple network segments or routers that contain overlapping IP address ranges.

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 Extreme Security input sources.

For information about assigning your network to pre-configured domains, see Network hierarchy on page 63.

Precedence order for evaluating domain criteria

When events and flows come into the Extreme Security 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 the domain is defined based on a flow, which is available only in Extreme SIEM deployments, the following order of precedence is applied:

1. flow source
2. flow 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 Extreme Security system

Domain information is removed when data is forwarded to another Extreme Security system. Events and flows that contain domain information are automatically assigned to the default domain on the receiving Extreme Security system. To identify which events and flows are assigned to the default domain, you can create a custom search on the receiving system. You might want to reassign these events and flows 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 flow source or flow collector, click the **Flows** 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.

   Important
   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 63.

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 offenses, assets, events, and flows 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:

User-defined domains
: You can create domains that are based on input sources by using the Domain Management tool. For more information, see *Creating domains*. Creating domains.

Default domain
: Everything that is not assigned to a user-defined domain is automatically assigned to the default domain. The default domain contains system-wide events.

> Important
> 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, flows, assets, and offenses . 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 and offenses

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.

In an Extreme Networks Security Analytics system that does not have user-defined domains, a rule creates an offense and keeps contributing to it each time the rule fires. In a domain-aware environment, a rule creates a new offense each time the rule is triggered in the context of a different domain.

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. An Any Domain rule creates an Any Domain offense.

Single-domain rule
: If the rule is a stateful rule, the states are maintained separately for each domain. When the rule is triggered, offenses are created separately for each domain that is involved and the offenses are tagged with those domains.

Single-domain offense
: The offense is tagged with the corresponding domain name. It can contain only events that are tagged with that 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. When the rule runs, it creates or contributes to a single system-wide offense.

System-wide offense
: The offense is tagged with Any Domain. It contains only events that are tagged with all domains.

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.

This two-column table shows examples of domain-aware rules and the behavior of the rule when it fires.

Table 62: 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.
domain is one of: Any Domain	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 `Any Domain`.

Table 62: Domain-aware rules (continued)

Domain text	Explanation	Rule response
domain is one of: Any Domain and a stateful test that is defined as when HTTP flow is detected 10 times within 1 minute	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 `Any Domain`. For example, if it detects 3 events that are tagged with `Domain_A`, 3 events that are tagged with `Domain_B`, and 4 events that are tagged with `Domain_C` within 1 minute, it creates an offense because it detected 10 events in total.
domain is one of: Any Domain, Domain_A	Works the same as a rule that has domain is one of: Any Domain.	When the domain test includes `Any Domain`, any single domains that are listed are ignored.

When you view the offense table, you can sort the offenses by clicking the Domain column. The Default Domain is not included in the sort function so it does not appear in alphabetical order. However, it appears at the top or bottom of the Domain list, depending on whether the column is sorted in ascending or descending order. Any Domain does not appear in the list of offenses.

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.

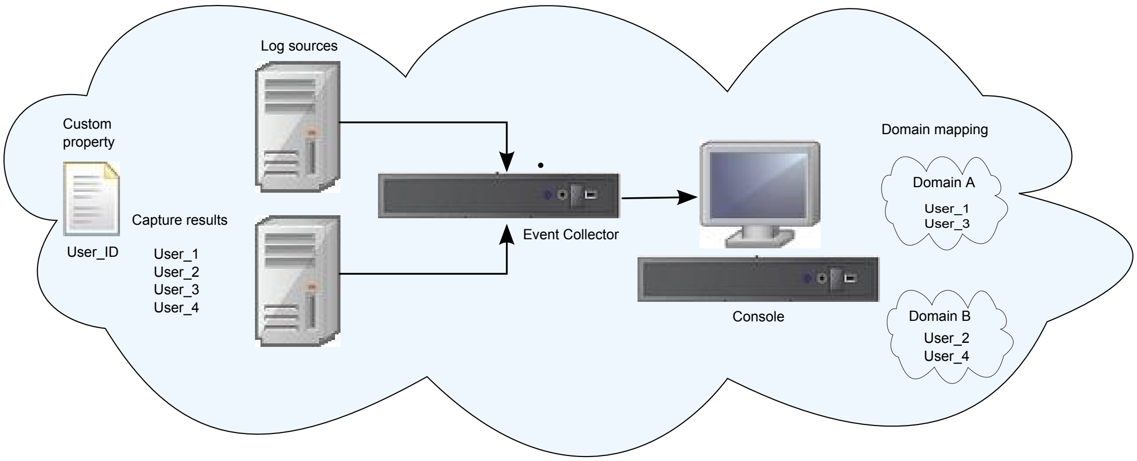

Figure 2: Assigning domains by using custom event property

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.

Important

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.

16 Asset growth deviations

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. Extreme Security uses the asset model to connect offenses in your deployment to physical or virtual assets in your network. 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.q1labs.assetprofile.updateresolution.UpdateResolutionManager:
[INFO] [NOT:0010006101][9.21.118.83/- -] [-/- -]
The top five most frequently deviating asset profiles between
Feb 13, 2015 8:10:23 PM AST and Feb 13, 2015 8:13:23 PM AST:
[ASSET ID:1003, REASON:Too Many IPs, COUNT:508],
[ASSET ID:1002, REASON:Too many DNS Names, COUNT:93],
[ASSET ID:1001, REASON:Too many MAC Addresses, COUNT:62]
```

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

Required user action

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

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

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

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

Related Links

Stale asset data on page 183

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 188

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 191

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 67

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 and flows, 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 185

Tuning the number of IP addresses allowed for a single asset on page 186

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 63: 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 184

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 64: 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 184

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 186

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)>` x `<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 185

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 15

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 65: 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 on page 103

Using the Reference Set Management window, you can create and manage reference sets. You can also import elements into a reference set from an external file.

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 66: Command syntax to modify asset blacklist and whitelist data

Name	Command syntax

Asset Reconciliation IPv4 Blacklist	`ReferenceSetUtil.sh add "Asset Reconciliation IPv4 Blacklist"` *`IP`*
	For example, this command adds IP address 192.168.3.56 to the blacklist:
	`ReferenceSetUtil.sh add "Asset Reconciliation IPv4 Blacklist" 192.168.3.56`

Asset Reconciliation DNS Blacklist	`ReferenceSetUtil.sh add "Asset Reconciliation DNS Blacklist"` *`DNS`*
	For example, this command adds domain name 'misbehaving.asset.company.com' to the blacklist:
	`ReferenceSetUtil.sh add "Asset Reconciliation DNS Blacklist" "misbehaving.asset.company.com"`

Table 66: Command syntax to modify asset blacklist and whitelist data (continued)

Name	Command syntax

Asset Reconciliation NetBIOS Blacklist	`ReferenceSetUtil.sh add "Asset Reconciliation NetBIOS Blacklist"` *`NETBIOS`*
	For example, this command removes NetBIOS host name 'deviantGrowthAsset-156384' from the blacklist:
	`ReferenceSetUtil.sh delete "Asset Reconciliation NetBIOS Blacklist" "deviantGrowthAsset-156384"`

Asset Reconciliation MAC Blacklist	`ReferenceSetUtil.sh add "Asset Reconciliation MAC Blacklist"` *`MACADDR`*
	For example, this command adds MAC address '00:a0:6b:54:9f:0e' to the blacklist:
	`ReferenceSetUtil.sh add "Asset Reconciliation MAC Blacklist" "00:a0:6b:54:9f:0e"`

Asset Reconciliation IPv4 Whitelist	`ReferenceSetUtil.sh add "Asset Reconciliation IPv4 Whitelist"` *`IP`*
	For example, this command deletes IP address 10.1.95.142 from the whitelist:
	`ReferenceSetUtil.sh delete "Asset Reconciliation IPv4 Whitelist" 10.1.95.142`

Asset Reconciliation DNS Whitelist	`ReferenceSetUtil.sh add "Asset Reconciliation DNS Whitelist"` *`DNS`*
	For example, this command adds domain name 'loadbalancer.company.com' to the whitelist:
	`ReferenceSetUtil.sh add "Asset Reconciliation DNS Whitelist" "loadbalancer.company.com"`

Asset Reconciliation NetBIOS Whitelist	`ReferenceSetUtil.sh add "Asset Reconciliation NetBIOS Whitelist"` *`NETBIOS`*
	For example, this command adds NetBIOS name 'assetName-156384' to the whitelist:
	`ReferenceSetUtil.sh add "Asset Reconciliation NetBIOS Whitelist" "assetName-156384"`

Asset Reconciliation MAC Whitelist	`ReferenceSetUtil.sh add "Asset Reconciliation MAC Blacklist"` *`MACADDR`*
	For example, this command adds MAC address '00:a0:6b:54:9f:0e' to the blacklist:
	`ReferenceSetUtil.sh add "Asset Reconciliation MAC Blacklist" "00:a0:6b:54:9f:0e"`

Related Links

Updating the blacklists and whitelists using the RESTful API on page 192

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 67: 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 191

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.

17 Configuring Extreme Security systems to forward data to other systems

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 and flows that contain domain information are automatically assigned to the default domain on the receiving system.

To avoid compatibility problems when sending event and flow 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 68: Forwarding Destinations parameters

Parameter	Description
Event Format	• Payload is the data in the format that the log source or flow source sent. • Normalized is raw data that is parsed and prepared as readable information for the user interface.
Destination Address	The IP address or host name of the vendor system that you want to forward data to.
Protocol	• TCP Use the TCP protocol to send normalized data by using the TCP protocol, you must create an off-site source at the destination address on port 32004. • UDP
Prefix a syslog header if it is missing or invalid	If a valid syslog header is not detected on the original syslog message, select this check box. The prefixed syslog header includes the Extreme SIEM appliance host IP address in the Hostname field of the syslog header. If this check box is not selected, the data is sent unmodified. When Extreme Security forwards syslog messages, the outbound message is verified to ensure that it has a valid syslog header.

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 SIEM 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 or flow 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 69: Routing Rules window parameters

Parameter	Description
Forwarding Event Collector	This option is displayed when you select the Online 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 Offline option. Specifies the Event Processor that you want this routing rule process data from. Restriction This option is not available if Drop is selected from the Routing Options pane.
Routing Options	• The Forward 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). • The Drop 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 Offline option. • The Bypass Correlation 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 Offline option. You can combine two options: • Forward and Drop Data is forwarded to the specified forwarding destination. Data is not stored in the database and is processed by the CRE. • Forward and Bypass Correlation 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. 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.

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 From the Data Source field in the Event Filters section, select which data source you want to route: Events or Flows.

   If you select the Flow Filters option, the section title changes to Flow Filters and the Match All Incoming Events check box changes to Match All Flows.

   e To forward all incoming data, select the Match All Incoming Events or Match All Incoming Flows check box.

   Restriction
   If you select this check box, you cannot add a filter.

   f To add a filter, in the Event Filters or Flow Filters section, select a filter from the first list and an operand from the second list.

   g In the text box, type the value that you want to filter for, and then click Add Filter.

   h Repeat the previous two steps for each filter that you want to add.

   i 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.

   Restriction
   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 see the *User Guide* for your product.

1 Click the Offenses Log Activity tab.

2 On the navigation 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 and flows that were seen for this forwarding destination.
- The number of events or flows that were sent to this forwarding destination.
- The number of events or flows 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 and flows that were seen for this forwarding destination.
   - The number of events or flows that were sent to this forwarding destination.
   - The number of events or flows that were dropped before the forwarding destination was reached.

4 On the toolbar, click an action, as described in the following table.

Table 70: 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.

18 Event store and forward

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 *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 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 71: Store and Forward window parameters

Parameter	Description
Display	The Schedules option shows a hierarchy of the parent-child relationship between the schedules, Event Processors and the associated Extreme Security Event Collectors. The Event Collectors option shows the lowest level in the hierarchy, which is a list of Extreme Security Event Collectors. Event Processors option shows a hierarchy of the parent-child relationship between the Event Processors and the associated Extreme Security Event Collectors.
Name	For the Schedules option, the Name column is displayed the following format. • First Level represents the name of the schedule. • Second Level represents the name of the Event Processor. • Third Level represents the name of the Event Collector. For the Event Processors option, the column is displayed in the following format • First Level represents the name of the Event Processor. • Second Level represents the name of the Event Collector. Tip 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.

Table 71: Store and Forward window parameters (continued)

Parameter	Description
Schedule Name	Displays the name of the schedule for the **Event Collectors** or **Event Processors** options. If an Event Processor is associated with more than one schedule, the **Schedule Name** shows **`Multiple`***n*, where *n* is the number of schedules. Tip Click the plus symbol (+) to view the associated schedules.
Last Status	Displays the status of the Store and Forward process: • **Forwarding** indicates that event forwarding is in progress. • **Forward Complete** 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. • **Warn** 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. • **Error** indicates that event forwarding was stopped before all stored events were forwarded. • **Inactive** indicates that no Extreme Security Event Collectors are assigned to the schedule, or the assigned Extreme Security Event Collectors are not receiving any events. Tip Move your mouse pointer over the **Last Status** column to view a summary of the status.
Forwarded Events	Displays the number of events (in K, M, or G) forwarded in the current session. Tip Move your mouse pointer over the value in the **Forwarded Events** column to view the number of events.
Remaining Events	Displays the number of events (in K, M, or G) remaining to be forwarded in the current session. Tip Move your mouse pointer over the value in the **Remaining Events** column to view the number of events.
Average Event Rate	Displays the average rate at which events are forwarding from the Event Collector to the Event Processor. Tip Move your mouse pointer over the value in the **Average Event Rate** column to view the average events per second (EPS).

Table 71: 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 Tip Move your mouse pointer over the value in the Current Event Rate 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.

19 Content Management Tool overview

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 SIEM system.

This technical note is intended for use by Customer Support, Professional Services, and select customers with advanced Extreme SIEM knowledge.

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
  - Flow 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 72: Parameters for CMT

Parameter	Description

`-h [--help]`
`ACTIONTYPE`
	Displays help that is specific to the ACTIONTYPE option or general help message if no ACTIONTYPE option is specified.

`-q [--quiet]`	No output appears on screen when CMT runs.
`-v [--verbose]`	Use verbose level when you log in to view default-level CMT information.
`-d [--debug]`	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 73: 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/qradar/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 74: 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 Content types.
`-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 `All` to export all content of the provided content-type.
`-g`	Include accumulated data in the export.

Table 75: Content types

Custom Content Type	Text String	Numeric Identifier
All custom content	`all`	n/a
Custom list of content	`package`	n/a
Dashboard	`dashboard`	4
Reports	`report`	10
Saved Searches	`search`	1
FGroup[1]	`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

[1] An FGroup represents a group of content within Extreme SIEM, such as a log source group, reporting group, or search group. These groups can be log activity event search groups, flow search groups, offense groups, asset 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 76: Search parameters

Parameter	Description
`-c or --content-type` *`content-type`*	The text string or numeric identifier of the type of content to export. The value can be anything from the content type table.
`-r or --regex` *`regex`*	The regular expression (regex) is used to search a content-type. All matching content is displayed.

Table 77: 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 78: Export parameters (multiple custom content items)

Parameter	Description
`-a [--action] export`	The action to be executed.
`-c [--content-type] package`	The content type to be exported. The "package" option is the required content-type.
`- f [--file] FILE`	The file path and file name, such as `/root/myPackage` 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.
`-o [-output-directory] PATH`	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/qradar/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 79: Export parameters (single content item)

Parameters	Description
`-o` *`directory_path`*	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.
`-c` *`content_type`*	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 Content Types.
`-a`	Specifies whether you want to export the specified custom content.
`-i` *`string_ID_value`*	The identifier for the specific instance of custom content, such as a single report or a single reference set. You can locate the `string_ID_value` 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 exported custom content into the same Extreme SIEM system that you exported from or another QRadar SIEM system.

If you want to import the content into another Extreme SIEM 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 SIEM 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 SIEM 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 80: Import parameters

Parameter	Description
`-a`	The action to be executed.
`-f` *`export_file_path`*	The file that contains the exported content data. This file is either a compressed `tar.gz`, 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 81: 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 82: Update parameters

Parameter	Description
-a or **--action update**	Changes the information on the system.
-f or **--file**	The compressed `tar.gz` 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 83: Audit details

Action/Audit event name	Event name	Event description
ExportInitiated	Content Export Initiated	User initiated content export
ExportComplete Note Also includes list of arguments that are exported in the audit output	Content Export Complete	Content export is complete
ImportInitiated	Content Import Initiated	User initiated content import

Table 83: 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 84: 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

20 SNMP trap configuration

In Extreme Networks Security Analytics, you can configure a rule to generate a rule response that sends an SNMP trap when configured conditions are met. Extreme Security 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 Extreme Security 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. Extreme Security 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/) 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.

Restriction
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 and flows 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 85: Value types for variable binding

Value type	Description	Example
`string`	Alphanumeric characters You can configure multiple values.	

`integer32`	A numerical value	`name="ATTACKER_PORT"`
		`type="integer32">%ATTACKER_PORT%`

`oid`	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"`
`gauge32`	A numerical value range	
`counter64`	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 86: Fields for the variable bindings

Field	Description	Example
`Native`	For more information about these fields, see the `/opt/qradar/conf/snmp.help` file.	Example [1]If the value type is `ipAddress`, you must use a variable that is an IP address. The string value type accepts any format.
`Custom`	Custom SNMP trap information that you configured for the custom rules wizard	Example [1]If you used the default file information and want to include this information in the SNMP trap, include the following code: `<variableBinding name="My Color Variable Binding" OID="1.3.6.1.4.1.20212.3.1" type="string"> My favorite color is %MyColor%</variableBinding>`
[1]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 and flows 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 87: Attributes for the <include> element

Attribute	Description
`name`	Displayed in the list box
`uri`	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 and flows 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 88: Attribute values to update in the <trapConfig> element

Element	Description
`</snmpHost>`	The new host to which you want to send SNMP traps. The value for the`snmpVersion` attribute for `<snmpHost>` element must be 2 or 3.
`<communityString>`	The community string for the host
`<authentication>`	An authentication protocol, security level, and password for the host.
`<decryption>`	The decryption protocol and password for the host.
`<user>`	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 and flows stops until the deployment completes.

21 Data obfuscation

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.

Restriction
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 Networks SIEM 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 89: Command options for generating the RSA private key

Option	Description
[**-out** *filename*]	The file name of the RSA private key file
[**numbits**]	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 90: Options to format the private key

Option	Description
[**-topk8**]	Reads a traditional format private key and writes the private key in PKCS #8 format
[**-inform**]	The input format of the private key as Privacy Enhanced Mail (`.PEM`) Example `-inform PEM`

Table 90: Options to format the private key (continued)

Option	Description
[-**outform**]	The format of the private key output as `.PEM` Example `-outform PEM`
[-**in** *filename*]	The file name for the private key
[-**out***filename*]	The output file name
[-**nocrypt**]	Specifies that the private key uses the unencrypted **PrivateKeyInfo** 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 91: Command options for generating the public key

Option	Description
[-**in** *filename*]	Specifies the input file name
[-**pubout**]	Generates a public key
[-**outform** DER]	The type of the public key file as DER Encoded X509 Certificate file (.DER)
[-**out** *filename*]	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
```

Restriction

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.

Restriction

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 92: 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 ***Log Source*** type. Identifies the event and extract the data to be obfuscated.	[1]*sensordeviceType*
<deviceId>	Identifies the ***Log Source***. Identifies the event and extract the data to be obfuscated.	[1]*sensordevice*
<qidId>	Identifies the ***Event*** name. Identifies the event and extract the data to obfuscate.	[1]*qidmap*
<category>	Identifies the low-level ***Category of the Event***. Identifies the event and extract the data to be obfuscated.	[1]*Type*
<enabled>	If true, enables the regular expression. If false, disables the regular expression.	

[1]You can configure a value of **-1** 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>
        <deviceTypeId>-1</deviceTypeId>
        <deviceId>-1</deviceId>
        <qidId>-1</qidId>
        <category>-1</category>
        <enabled>false</enabled>
    </expression>
</ObfuscationExpressions>
```

3 The following example shows the regular expressions that can parse user names.

Table 93: Example regex patterns that can parse user names

<table>
<tr><th>Example regex patterns</th><th>Matches</th></tr>
<tr><td>usrName=([0-9a-zA-Z]([-.\w]*[0-9a-zA-Z])*@([0-9a-zA-Z][-\w]*[0-9a-zA-Z]\.)+[a-zA-Z]{2,20})$</td><td>john_smith@IBM.com, jon@ibm.com, jon@us.ibm.com</td></tr>
<tr><td>usrName=(^([\w]+[^\W])([^\W]\.?)([\w]+[^\W]$))</td><td>john.smith, John.Smith, john, jon_smith</td></tr>
<tr><td>usrName=^([a-zA-Z])[a-zA-Z_-]*[\w_-]*[\S]$|^([a-zA-Z])[0-9_-]*[\S]$|^[a-zA-Z]*[\S]$</td><td>johnsmith, Johnsmith123, john_smith123, john123_smith, john-smith</td></tr>
<tr><td>usrName=(/S+)</td><td>Matches any non-white space after the equal, =, sign. This greedy regular expression can lead to system performance issues.</td></tr>
<tr><td>msg=([0-9a-zA-Z]([-.\w]*[0-9a-zA-Z]))*@\b(([01]?\d?\d|2[0-4]\d|25[0-5])\.){3}([01]?\d?\d|2[0-4]\d|25[0-5])\b</td><td>Matches users with IP address.
Example
john.smith@1.1.1.1</td></tr>
<tr><td>src=\b(([01]?\d?\d|2[0-4]\d|25[0-5])\.){3}([01]?\d?\d|2[0-4]\d|25[0-5])\b</td><td>Matches IP address formats.</td></tr>
<tr><td>host=^(([a-zA-Z0-9]|[a-zA-Z0-9][a-zA-Z0-9\-]*[a-zA-Z0-9])\.)*([A-Za-z0-9]|[A-Za-z0-9][A-Za-z0-9\-]*[A-Za-z0-9])$</td><td>hostname.ibm.com, hostname.co.uk,</td></tr>
</table>

Decrypting obfuscated data

When data obfuscation is configured on an Extreme SIEM 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.

1 Log in to the Extreme SIEM user interface and copy the obfuscated text that you want to decrypt

2 Using SSH, log in to your Extreme Security Console as the root user.

User name: `root`

3 Create a directory and copy the public and private keys to this directory.

4 Go to the directory where the keys are located.

5 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 94: Options for the `obfuscation_decoder.sh` script

Option	Description
-**k publickey** *filename*	The public key file name
-**p privatekey** *filename*	The private key file name
-**d obfuscated** *text*	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:

1 Log in to the Extreme Security Console.

2 Click the Assets tab.

3 To remove unobfuscated hosts and user names, click Actions > Delete Listed.

4 Run scan profile manually or run schedule the scan profile to run.

5 To repopulate the data for building blocks on your Extreme Security system, run the Server Discovery tool.

22 Audit logs

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 95: Description of the parts of the log file format

File format part	Description
date_time	The date and time of the activity in the format: Month Date HH:MM:SS
host name	The host name of the Console where this activity was logged.
user	The name of the user who changed the settings.
IP address	The IP address of the user who changed the settings.
thread ID)	The identifier of the Java™ thread that logged this activity.
category	The high-level category of this activity.
sub-categor	The low-level category of this activity.

Table 95: Description of the parts of the log file format (continued)

File format part	Description
`action`	The activity that occurred.
`payload`	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 int 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:

Administrator Authentication	• Log in to the Administration Console • Log out of the Administration Console.
Assets	• Delete an asset. • Delete all assets.
Audit Log Access	A search that includes events that have a high-level event category of Audit.
Backup and Recovery	• Edit the configuration. • Initiate the backup. • Complete the backup. • Fail the backup. • Delete the backup. • Synchronize the backup. • Cancel the backup. • Initiate the restore. • Upload a backup. • Upload an invalid backup. • Initiate the restore. • Purge the backup.
Custom Properties	• Add a custom event property. • Edit a custom event property. • Delete a custom event property. • Edit a custom flow property. • Delete a custom flow property.
Chart Configuration	Save flow or event chart configuration.

Custom Property Expressions	• Add a custom event property expression. • Edit a custom event property expression. • Delete a custom event property expression. • Add a custom flow property expression. • Edit a custom flow property expression. • Delete a custom flow property expression.
Retention Buckets	• Add a bucket. • Delete a bucket. • Edit a bucket. • Enable or disable a bucket.
Flow Sources	• Add a flow source. • Edit a flow source. • Delete a flow source.
Groups	• Add a group. • Delete a group. • Edit a group.
High Availability	• Add a license key. • Revert a license. • Delete a license key.
Log Source Extension	• Add an log source extension. • Edit the log source extension. • Delete a log source extension. • Upload a log source extension. • Upload a log source extension successfully. • Upload an invalid log source extension. • Download a log source extension. • Report a log source extension. • Modify a log sources association to a device or device type.
Offenses	• Hide an offense. • Close an offense. • Close all offenses. • Add a destination note. • Add a source note. • Add a network note. • Add an offense note. • Add a reason for closing offenses. • Edit a reason for closing offenses.
Protocol Configuration	• Add a protocol configuration. • Delete a protocol configuration. • Edit a protocol configuration.
QIDmap	• Add a QID map entry. • Edit a QID map entry.

Vulnerability Manager	• Create a scanner schedule. • Update a scanner schedule. • Delete a scanner schedule. • Start a scanner schedule. • Pause a scanner schedule. • Resume a scanner schedule.
Reference Sets	• Create a reference set. • Edit a reference set. • Purge elements in a reference set. • Delete a reference set. • Add reference set elements. • Delete reference set elements. • Delete all reference set elements. • Import reference set elements. • Export reference set elements.
Reports	• Add a template. • Delete a template. • Edit a template. • Generate a report. • Delete a report. • Delete generated content. • View a generated report. • Email a generated report.
Root Login	• Log in to Extreme Security, as root. • Log out of Extreme Security, as root.
Rules	• Add a rule. • Delete a rule. • Edit a rule.
Scanner	• Add a scanner. • Delete a scanner. • Edit a scanner.
Scanner Schedule	• Add a schedule. • Edit a schedule. • Delete a schedule.
Session Authentication	• Create an administration session. • Terminate an administration session. • Deny an invalid authentication session. • Expire a session authentication. • Create an authentication session. • Terminate an authentication session
SIM	Clean a SIM model.
Store and Forward	• Add a Store and Forward schedule. • Edit a Store and Forward schedule. • Delete a Store and Forward schedule.

Syslog Forwarding	• Add a syslog forwarding. • Delete a syslog forwarding. • Edit a syslog forwarding.
System Management	• Shut down a system. • Restart a system.
User Accounts	• Add an account. • Edit an account. • Delete an account.
User Authentication	• Log in to the user interface. • Log out of the user interface.
User Authentication Ariel	• Deny a login attempt. • Add an Ariel property. • Delete an Ariel property. • Edit an Ariel property. • Add an Ariel property extension. • Delete an Ariel property extension. • Edit an Ariel property extension.
User Roles	• Add a role. • Edit a role. • Delete a role.
VIS	• Discover a new host. • Discover a new operating system. • Discover a new port. • Discover a new vulnerability.

23 Event categories

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 96: High-level event categories

Category	Description
Recon on page 235	Events that are related to scanning and other techniques that are used to identify network resources, for example, network or host port scans.
DoS on page 235	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.
Authentication on page 238	Events that are related to authentication controls, group, or privilege change, for example, log in or log out.
Access on page 242	Events resulting from an attempt to access network resources, for example, firewall accept or deny.
Exploit on page 244	Events that are related to application exploits and buffer overflow attempts, for example, buffer overflow or web application exploits.
Malware on page 245	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.
Suspicious Activity on page 246	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.
System on page 248	Events that are related to system changes, software installation, or status messages.
Policy on page 251	Events regarding corporate policy violations or misuse.
Unknown on page 252	Events that are related to unknown activity on your system.
CRE on page 253	Events that are generated from an offense or event rule.
Potential Exploit on page 253	Events relate to potential application exploits and buffer overflow attempts.
User Defined on page 254	Events that are related to user-defined objects.
SIM Audit on page 256	Events that are related to user interaction with the Console and administrative functions.
VIS Host Discovery on page 256	Events that are related to the host, ports, or vulnerabilities that the VIS component discovers.
Application on page 257	Events that are related to application activity.
Audit on page 272	Events that are related to audit activity.
Risk on page 272	Events that are related to risk activity in Extreme Networks Security Risk Manager.
Risk Manager Audit on page 273	Events that are related to audit activity in Extreme Networks Security Risk Manager.
Control on page 274	Events that are related to your hardware system.
Asset Profiler on page 275	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 97: 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 98: 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
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

Table 98: Low-level categories and severity levels for the DoS events category (continued)

Low-level event category	Description	Severity level (0 - 10)
Distributed Medium Rate TCP DoS	Indicates a distributed medium rate TCP DoS attack.	8
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 99: 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 99: 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 99: 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 99: 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 99: 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 100: 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	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 100: 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 101: 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 101: 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 102: 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 102: 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 103: 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 103: 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 SIEM 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 103: 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 104: 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 104: 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 104: 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 105: 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 106: 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 Snort Event	Indicates an unknown Snort event.	3
Unknown Dragon Event	Indicates an unknown Dragon event.	3

Table 106: 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 a custom offense, flow, or event rule.

The following table describes the low-level event categories and associated severity levels for the CRE category.

Table 107: 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
Cross-Offense Event Sequence Rule Match	Indicates a cross-offense event sequence rule match.	5
Offense Rule Match	Indicates an offense 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 108: 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
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 109: 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

Table 109: Low-level categories and severity levels for the User Defined category (continued)

Low-level event category	Description	Severity level (0 - 10)
Custom Sentry 4	Indicates a custom anomaly event with a severity level of 4.	4
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 110: 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 111: 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

Table 111: Low-level categories and severity levels for the VIS host discovery category (continued)

Low-level event category	Description	Severity level (0 - 10)
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 112: 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

Table 112: Low-level categories and severity levels for the application category (continued)

Low-level event category	Description	Severity level (0 - 10)
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
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

Table 112: Low-level categories and severity levels for the application category (continued)

Low-level event category	Description	Severity level (0 - 10)
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
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

Table 112: Low-level categories and severity levels for the application category (continued)

Low-level event category	Description	Severity level (0 - 10)
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
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

Table 112: Low-level categories and severity levels for the application category (continued)

Low-level event category	Description	Severity level (0 - 10)
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
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

Table 112: Low-level categories and severity levels for the application category (continued)

Low-level event category	Description	Severity level (0 - 10)
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
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

Table 112: Low-level categories and severity levels for the application category (continued)

Low-level event category	Description	Severity level (0 - 10)
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 an IBM® 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
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

Table 112: Low-level categories and severity levels for the application category (continued)

Low-level event category	Description	Severity level (0 - 10)
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
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

Table 112: Low-level categories and severity levels for the application category (continued)

Low-level event category	Description	Severity level (0 - 10)
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
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

Table 112: Low-level categories and severity levels for the application category (continued)

Low-level event category	Description	Severity level (0 - 10)
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
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

Table 112: Low-level categories and severity levels for the application category (continued)

Low-level event category	Description	Severity level (0 - 10)
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
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

Table 112: Low-level categories and severity levels for the application category (continued)

Low-level event category	Description	Severity level (0 - 10)
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
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

Table 112: Low-level categories and severity levels for the application category (continued)

Low-level event category	Description	Severity level (0 - 10)
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
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

Table 112: Low-level categories and severity levels for the application category (continued)

Low-level event category	Description	Severity level (0 - 10)
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
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

Table 112: Low-level categories and severity levels for the application category (continued)

Low-level event category	Description	Severity level (0 - 10)
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
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

Table 112: Low-level categories and severity levels for the application category (continued)

Low-level event category	Description	Severity level (0 - 10)
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 113: 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 114: 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
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 confidentially 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 115: 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 116: 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

Table 116: Low-level categories and severity levels for the control category (continued)

Low-level event category	Description	Severity level (0 - 10)
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 117: 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

Table 117: Low-level categories and severity levels for the asset profiler category (continued)

Low-level event category	Description	Severity level (0 - 10)
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
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

Table 117: Low-level categories and severity levels for the asset profiler category (continued)

Low-level event category	Description	Severity level (0 - 10)
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
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

Table 117: Low-level categories and severity levels for the asset profiler category (continued)

Low-level event category	Description	Severity level (0 - 10)
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

24 Ports used by Extreme Security

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. Extreme Security QFlow Collectors that use encryption can initiate SSH sessions to Flow Processor appliances that require data.

SIEM 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.

The following table lists the ports, protocols, communication direction, description, and the reason that the port is used.

Table 118: 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 118: 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	WinCollect agents and Windows operating systems that are remotely polled for events. 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. Bidirectional traffic between Adaptive Log Exporter agents and Windows operating systems that are remotely polled for events.	This traffic is generated by WinCollect, Microsoft Security Event Log Protocol, or Adaptive Log Exporter. Note 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.
137	Windows NetBIOS name service	UDP	Bidirectional traffic between WinCollect agents and Windows operating systems that are remotely polled for events 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. Bidirectional traffic between Adaptive Log Exporter agents and Windows operating systems that are remotely polled for events	This traffic is generated by WinCollect, Microsoft Security Event Log Protocol, or Adaptive Log Exporter.

Table 118: Listening ports that are used by QRadar, services, and components (continued)

Port	Description	Protocol	Direction	Requirement
138	Windows NetBIOS datagram service	UDP	Bidirectional traffic between WinCollect agents and Windows operating systems that are remotely polled for events 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. Bidirectional traffic between Adaptive Log Exporter agents and Windows operating systems that are remotely polled for events	This traffic is generated by WinCollect, Microsoft Security Event Log Protocol, or Adaptive Log Exporter. .
139	Windows NetBIOS session service	TCP	Bidirectional traffic between WinCollect agents and Windows operating systems that are remotely polled for events 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. Bidirectional traffic between Adaptive Log Exporter agents and Windows operating systems that are remotely polled for events	This traffic is generated by WinCollect, Microsoft Security Event Log Protocol, or Adaptive Log Exporter.
199	NetSNMP	TCP	Extreme Security managed hosts that connect to the Extreme Security Console External log sources to Extreme Security Extreme Security Event Collectors	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.

Table 118: Listening ports that are used by QRadar, services, and components (continued)

Port	Description	Protocol	Direction	Requirement
443	Apache/HTTPS	TCP	Bidirectional traffic for secure communications from all products to the Extreme Security Console	Configuration downloads to managed hosts from the Extreme Security Console Extreme Security managed hosts that connect to the Extreme Security Console Users to have log in access to Extreme Security Extreme Security Console that manage and provide configuration updates for WinCollect agents
445	Microsoft Directory Service	TCP	Bidirectional traffic between WinCollect agents and Windows operating systems that are remotely polled for events 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 Bidirectional traffic between Adaptive Log Exporter agents and Windows operating systems that are remotely polled for events	This traffic is generated by WinCollect, Microsoft Security Event Log Protocol, or Adaptive Log Exporter.
514	Syslog	UDP/TCP	External network appliances that provide TCP syslog events use bidirectional traffic. External network appliances that provide UDP syslog events use uni-directional traffic.	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

Table 118: Listening ports that are used by QRadar, services, and components (continued)

Port	Description	Protocol	Direction	Requirement
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.
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 **Admin** 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

Table 118: Listening ports that are used by QRadar, services, and components (continued)

Port	Description	Protocol	Direction	Requirement
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 Note These ports are used by Extreme Security support.
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
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

Table 118: Listening ports that are used by QRadar, services, and components (continued)

Port	Description	Protocol	Direction	Requirement
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
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

Table 118: Listening ports that are used by QRadar, services, and components (continued)

Port	Description	Protocol	Direction	Requirement
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	Collecting incoming packet capture (PCAP) data from Juniper Networks SRX Series appliances. Note 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
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.

> Important
> 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.

25 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 and that Extreme Security accesses.

Table 119: Public servers that Extreme Security must access

IP address or hostname	Description
194.153.113.31	Extreme Security Vulnerability Manager DMZ scanner
194.153.113.32	Extreme Security Vulnerability Manager DMZ scanner
qmmunity.q1labs.com	Extreme Security auto-update server
www.iss.net	X-Force Threat Information Center dashboard item
update.xforce-security.com	X-Force Threat Feed update server
license.xforce-security.com	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 120: RSS feeds

Title	URL	Requirements
Security Intelligence	http://feeds.feedburner.com/SecurityIntelligence	Extreme Security and an Internet connection
Security Intelligence Vulns / Threats	http://securityintelligence.com/topics/ vulnerabilities-threats/feed	Extreme Security and an Internet connection
IBM My Notifications	http://www-945.events.ibm.com/systems/support/ myfeed/xmlfeeder.wss?feeder.requid= feeder.create_feed&feeder.feedtype=RSS&feeder.uid=270006EH0R&feeder.subscrid= S14b5f284d32&feeder.subdefkey=swgother&feeder. maxfeed=25	Extreme Security and an Internet connection
Security News	http://*IP_address_of_QVM_processor* :8844/rss/research/news.rss	Vulnerability Manager processor is deployed
Security Advisories	http://*IP_address_of_QVM_processor* :8844/rss/research/advisories.rss	Vulnerability Manager processor is deployed
Latest Published Vulnerabilities	http://*IP_address_of_QVM_processor* :8844/rss/research/vulnerabilities.rss	Vulnerability Manager processor deployed

Table 120: RSS feeds (continued)

Title	URL	Requirements
Scans Completed	http://*IP_address_of_QVM_processor*:8844/rss/scanresults/completedScans.rss	Vulnerability Manager processor is deployed
Scans In Progress	http://*IP_address_of_QVM_processor*:8844/rss/scanresults/runningScans.rss	Vulnerability Manager processor is deployed

Glossary

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 IBM Terminology website (opens in new window).

A on page 291 B on page 291 C on page 292 D on page 292 E on page 292 F on page 293 G on page 293 H on page 293 I on page 294 K on page 294 L on page 294 M on page 295 N on page 295 O on page 295 P on page 296 Q on page 296 R on page 296 S on page 297 T on page 297 V on page 298 W on page 298

A

accumulator	A register in which one operand of an operation can be stored and subsequently replaced by the result of that operation.
active system	In a high-availability (HA) cluster, the system that has all of its services running.
Address Resolution Protocol (ARP)	A protocol that dynamically maps an IP address to a network adapter address in a local area network.
administrative share	A network resource that is hidden from users without administrative privileges. Administrative shares provide administrators with access to all resources on a network system.
anomaly	A deviation from the expected behavior of the network.
application signature	A unique set of characteristics that are derived by the examination of packet payload and then used to identify a specific application.
ARP	See Address Resolution Protocol.
ARP Redirect	An ARP method for notifying the host if a problem exists on a network.
ASN	See autonomous system number.
asset	A manageable object that is either deployed or intended to be deployed in an operational environment.
autonomous system number (ASN)	In TCP/IP, a number that is assigned to an autonomous system by the same central authority that assigns IP addresses. The autonomous system number makes it possible for automated routing algorithms to distinguish autonomous systems.

B

behavior	The observable effects of an operation or event, including its results.
bonded interface	See link aggregation.
burst	A sudden sharp increase in the rate of incoming events or flows such that the licensed flow or event rate limit is exceeded.

C

CIDR
See Classless Inter-Domain Routing.

Classless Inter-Domain Routing (CIDR)
A method for adding class C Internet Protocol (IP) addresses. The addresses are given to Internet Service Providers (ISPs) for use by their customers. CIDR addresses reduce the size of routing tables and make more IP addresses available within organizations.

client
A software program or computer that requests services from a server.

cluster virtual IP address
An IP address that is shared between the primary or secondary host and the HA cluster.

coalescing interval
The interval at which events are bundled. Event bundling occurs in 10 second intervals and begins with the first event that does not match any currently coalescing events. Within the coalescing interval, the first three matching events are bundled and sent to the event processor.

Common Vulnerability Scoring System (CVSS)
A scoring system by which the severity of a vulnerability is measured.

console
A display station from which an operator can control and observe the system operation.

content capture
A process that captures a configurable amount of payload and then stores the data in a flow log.

credential
A set of information that grants a user or process certain access rights.

credibility
A numeric rating between 0-10 that is used to determine the integrity of an event or an offense. Credibility increases as multiple sources report the same event or offense.

CVSS
See Common Vulnerability Scoring System.

D

database leaf object
A terminal object or node in a database hierarchy.

datapoint
A calculated value of a metric at a point in time.

Device Support Module (DSM)
A configuration file that parses received events from multiple log sources and coverts them to a standard taxonomy format that can be displayed as output.

DHCP
See Dynamic Host Configuration Protocol.

DNS
See Domain Name System.

Domain Name System (DNS)
The distributed database system that maps domain names to IP addresses.

DSM
See Device Support Module.

duplicate flow
Multiple instances of the same data transmission received from different flow sources.

Dynamic Host Configuration Protocol (DHCP)
A communications protocol that is used to centrally manage configuration information. For example, DHCP automatically assigns IP addresses to computers in a network.

E

encryption
In computer security, the process of transforming data into an unintelligible form in such a way that the original data either cannot be obtained or can be obtained only by using a decryption process.

endpoint
The address of an API or service in an environment. An API exposes an endpoint and at the same time invokes the endpoints of other services.

external scanning appliance
A machine that is connected to the network to gather vulnerability information about assets in the network.

F

false positive
A test result classed as positive (indicating that the site is vulnerable to attack), that the user decides is in fact negative (not a vulnerability).

flow
A single transmission of data passing over a link during a conversation.

flow log
A collection of flow records.

flow sources
The origin from which flow is captured. A flow source is classified as internal when flow comes from hardware installed on a managed host or it is classified as external when the flow is sent to a flow collector.

forwarding destination
One or more vendor systems that receive raw and normalized data from log sources and flow sources.

FQDN
See fully qualified domain name.

FQNN
See fully qualified network name.

fully qualified domain name (FQDN)
In Internet communications, the name of a host system that includes all of the subnames of the domain name. An example of a fully qualified domain name is rchland.vnet.ibm.com.

fully qualified network name (FQNN)
In a network hierarchy, the name of an object that includes all of the departments. An example of a fully qualified network name is CompanyA.Department.Marketing.

G

gateway
A device or program used to connect networks or systems with different network architectures.

H

HA
See high availability.

HA cluster
A high-availability configuration consisting of a primary server and one secondary server.

Hash-Based Message Authentication Code (HMAC)
A cryptographic code that uses a cryptic hash function and a secret key.

high availability (HA)
Pertaining to a clustered system that is reconfigured when node or daemon failures occur so that workloads can be redistributed to the remaining nodes in the cluster.

HMAC
See Hash-Based Message Authentication Code.

host context
A service that monitors components to ensure that each component is operating as expected.

I

ICMP	See Internet Control Message Protocol.
identity	A collection of attributes from a data source that represent a person, organization, place, or item.
IDS	See intrusion detection system.
Internet Control Message Protocol (ICMP)	An Internet protocol that is used by a gateway to communicate with a source host, for example, to report an error in a datagram.
Internet Protocol (IP)	A protocol that routes data through a network or interconnected networks. This protocol acts as an intermediary between the higher protocol layers and the physical network. See also Transmission Control Protocol.
Internet service provider (ISP)	An organization that provides access to the Internet.
intrusion detection system (IDS)	Software that detects attempts or successful attacks on monitored resources that are part of a network or host system.
intrusion prevention system (IPS)	A system that attempts to deny potentially malicious activity. The denial mechanisms could involve filtering, tracking, or setting rate limits.
IP	See Internet Protocol.
IP multicast	Transmission of an Internet Protocol (IP) datagram to a set of systems that form a single multicast group.
IPS	See intrusion prevention system.
ISP	See Internet service provider.

K

key file	In computer security, a file that contains public keys, private keys, trusted roots, and certificates.

L

L2L	See Local To Local.
L2R	See Local To Remote.
LAN	See local area network.
LDAP	See Lightweight Directory Access Protocol.
leaf	In a tree, an entry or node that has no children.
Lightweight Directory Access Protocol (LDAP)	An open protocol that uses TCP/IP to provide access to directories that support an X.500 model and that does not incur the resource requirements of the more complex X.500 Directory Access Protocol (DAP). For example, LDAP can be used to locate people, organizations, and other resources in an Internet or intranet directory.
link aggregation	The grouping of physical network interface cards, such as cables or ports, into a single logical network interface. Link aggregation is used to increase bandwidth and network availability.
live scan	A vulnerability scan that generates report data from the scan results based on the session name.

local area network (LAN)	A network that connects several devices in a limited area (such as a single building or campus) and that can be connected to a larger network.
Local To Local (L2L)	Pertaining to the internal traffic from one local network to another local network.
Local To Remote (L2R)	Pertaining to the internal traffic from one local network to another remote network.
log source	Either the security equipment or the network equipment from which an event log originates.
log source extension	An XML file that includes all of the regular expression patterns required to identify and categorize events from the event payload.

M

magistrate	An internal component that analyzes network traffic and security events against defined custom rules.
magnitude	A measure of the relative importance of a particular offense. Magnitude is a weighted value calculated from relevance, severity, and credibility.

N

NAT	See network address translation.
NetFlow	A Cisco network protocol that monitors network traffic flow data. NetFlow data includes the client and server information, which ports are used, and the number of bytes and packets that flow through the switches and routers connected to a network. The data is sent to NetFlow collectors where data analysis takes place.
network address translation (NAT)	In a firewall, the conversion of secure Internet Protocol (IP) addresses to external registered addresses. This enables communications with external networks but masks the IP addresses that are used inside the firewall.
network hierarchy	A type of container that is a hierarchical collection of network objects.
network layer	In OSI architecture, the layer that provides services to establish a path between open systems with a predictable quality of service.
network object	A component of a network hierarchy.
network weight	The numeric value applied to each network that signifies the importance of the network. The network weight is defined by the user.

O

offense	A message sent or an event generated in response to a monitored condition. For example, an offense will provide information on whether a policy has been breached or the network is under attack.
offsite source	A device that is away from the primary site that forwards normalized data to an event collector.
offsite target	A device that is away from the primary site that receives event or data flow from an event collector.
Open Source Vulnerability Database (OSVDB)	Created by the network security community for the network security community, an open source database that provides technical information on network security vulnerabilities.

open systems interconnection (OSI)
The interconnection of open systems in accordance with standards of the International Organization for Standardization (ISO) for the exchange of information.

OSI
See open systems interconnection.

OSVDB
See Open Source Vulnerability Database.

P

parsing order
A log source definition in which the user can define the order of importance for log sources that share a common IP address or host name.

payload data
Application data contained in an IP flow, excluding header and administrative information.

primary HA host
The main computer that is connected to the HA cluster.

protocol
A set of rules controlling the communication and transfer of data between two or more devices or systems in a communication network.

Q

QID Map
A taxonomy that identifies each unique event and maps the events to low-level and high-level categories to determine how an event should be correlated and organized.

R

R2L
See Remote To Local.

R2R
See Remote To Remote.

recon
See reconnaissance.

reconnaissance (recon)
A method by which information pertaining to the identity of network resources is gathered. Network scanning and other techniques are used to compile a list of network resource events which are then assigned a severity level.

reference map
A data record of direct mapping of a key to a value, for example, a user name to a global ID.

reference map of maps
A data record of two keys mapped to many values. For example, the mapping of the total bytes of an application to a source IP.

reference map of sets
A data record of a key mapped to many values. For example, the mapping of a list of privileged users to a host.

reference set
A list of single elements that are derived from events or flows on a network. For example, a list of IP addresses or a list of user names.

reference table
A table where the data record maps keys that have an assigned type to other keys, which are then mapped to a single value.

refresh timer
An internal device that is triggered manually or automatically at timed intervals that updates the current network activity data.

relevance
A measure of relative impact of an event, category, or offense on the network.

Remote To Local (R2L)
The external traffic from a remote network to a local network.

Remote To Remote (R2R)
The external traffic from a remote network to another remote network.

report

In query management, the formatted data that results from running a query and applying a form to it.

report interval

A configurable time interval at the end of which the event processor must send all captured event and flow data to the console.

routing rule

A condition that when its criteria are satisfied by event data, a collection of conditions and consequent routing are performed.

rule

A set of conditional statements that enable computer systems to identify relationships and run automated responses accordingly.

S

scanner

An automated security program that searches for software vulnerabilities within web applications.

secondary HA host

The standby computer that is connected to the HA cluster. The secondary HA host assumes responsibility of the primary HA host if the primary HA host fails.

severity

A measure of the relative threat that a source poses on a destination.

Simple Network Management Protocol (SNMP)

A set of protocols for monitoring systems and devices in complex networks. Information about managed devices is defined and stored in a Management Information Base (MIB).

SNMP

See Simple Network Management Protocol.

SOAP

A lightweight, XML-based protocol for exchanging information in a decentralized, distributed environment. SOAP can be used to query and return information and invoke services across the Internet.

standby system

A system that automatically becomes active when the active system fails. If disk replication is enabled, replicates data from the active system.

subnet

See subnetwork.

subnet mask

For internet subnetworking, a 32-bit mask used to identify the subnetwork address bits in the host portion of an IP address.

subnetwork (subnet)

A network that is divided into smaller independent subgroups, which still are interconnected.

sub-search

A function that allows a search query to be performed within a set of completed search results.

superflow

A single flow that is comprised of multiple flows with similar properties in order to increase processing capacity by reducing storage constraints.

system view

A visual representation of both primary and managed hosts that compose a system.

T

TCP

See Transmission Control Protocol.

Transmission Control Protocol (TCP)

A communication protocol used in the Internet and in any network that follows the Internet Engineering Task Force (IETF) standards for internetwork protocol. TCP provides a reliable host-to-host protocol in packet-switched communication networks and in interconnected systems of such networks. See also Internet Protocol.

truststore file

A key database file that contains the public keys for a trusted entity.

V

violation An act that bypasses or contravenes corporate policy.

vulnerability A security exposure in an operating system, system software, or application software component.

W

whois server A server that is used to retrieve information about a registered Internet resources, such as domain names and IP address allocations.

Index