



# Extreme Networks SIEM Getting Started Guide

Copyright © 2016 All rights reserved.

## Legal Notice

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

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

## Trademarks

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

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

For additional information on Extreme Networks trademarks, please see:

[www.extremenetworks.com/company/legal/trademarks](http://www.extremenetworks.com/company/legal/trademarks)

## Support

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

For information, contact:

Extreme Networks, Inc.

145 Rio Robles

San Jose, California 95134

USA

# Table of Contents

---

- Introduction to getting started with Extreme SIEM..... 4**
  - Text Conventions.....4
  - Providing Feedback to Us.....5
  - Getting Help.....5
  - Related Publications.....6
  
- Chapter 1: Extreme SIEM overview..... 7**
  - Log activity.....7
  - Network activity.....7
  - Assets.....7
  - Offenses.....8
  - Reports.....8
  - Data collection.....8
  - Extreme SIEM rules.....10
  - Supported web browsers .....10
  
- Chapter 2: Getting started with Extreme SIEM deployment..... 11**
  - Installing the Extreme SIEM appliance.....11
  - The Extreme SIEM appliance.....11
  - Extreme SIEM configuration.....12
  - Extreme SIEM tuning.....15
  
- Chapter 3: Getting started in Extreme SIEM..... 19**
  - Searching events.....19
  - Saving event search criteria.....20
  - Configuring a time series chart.....20
  - Searching flows.....21
  - Saving flow search criteria.....21
  - Creating a dashboard item.....21
  - Searching assets.....22
  - Offense Investigations.....23
  - Example: Enabling the PCI report templates.....23
  - Example: Creating a custom report based on a saved search.....23



# Introduction to getting started with Extreme SIEM

This guide introduces you to key concepts, an overview of the installation process, and basic tasks that you perform in the user interface.

## Intended audience

This information is intended for use by security administrators who are responsible for investigating and managing network security. To use this guide you must have a knowledge of your corporate network infrastructure and networking technologies.






## Technical documentation

For information about how to access more technical documentation, technical notes, and release notes, see <http://documentation.extremenetworks.com>.

## Text Conventions

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

**Table 1: Notice Icons**

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

**Table 2: Text Conventions**

Convention	Description
<code>screen displays</code>	This typeface indicates command syntax, or represents information as it appears on the screen.
The words <b>enter</b> and <b>type</b>	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.”

**Table 2: Text Conventions (continued)**

Convention	Description
<b>[Key]</b> names	Key names are written with brackets, such as <b>[Return]</b> or <b>[Esc]</b> . If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press <b>[Ctrl]+[Alt]+[Del]</b>
<i>Words in italicized type</i>	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.

## 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](mailto:internalinfodev@extremenetworks.com).

## Getting Help

If you require assistance, contact Extreme Networks using one of the following methods:

- **Global Technical Assistance Center (GTAC) for Immediate Support**
  - **Phone:** 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: [www.extremenetworks.com/support/contact](http://www.extremenetworks.com/support/contact)
  - **Email:** [support@extremenetworks.com](mailto:support@extremenetworks.com). To expedite your message, enter the product name or model number in the subject line.
- **GTAC Knowledge** — Get on-demand and tested resolutions from the GTAC Knowledgebase, or create a help case if you need more guidance.
- **The Hub** — A forum for Extreme customers to connect with one another, get questions answered, share ideas and feedback, and get problems solved. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
- **Support Portal** — Manage cases, downloads, service contracts, product licensing, and training and certifications.

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

- Your Extreme Networks service contract number and/or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any action(s) already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load 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 related Return Material Authorization (RMA) numbers

## Related Publications

---

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

### ExtremeSecurity Analytics

- *Extreme Security Release Notes*
- *Extreme SIEM Administration Guide*
- *Extreme SIEM Getting Started Guide*
- *Extreme SIEM High Availability Guide*
- *Extreme SIEM User Guide*
- *Extreme SIEM Tuning Guide*
- *ExtremeSecurity API Reference Guide*
- *ExtremeSecurity Ariel Query Language Guide*
- *ExtremeSecurity Application Configuration Guide*
- *ExtremeSecurity DSM Configuration Guide*
- *ExtremeSecurity Hardware Guide*
- *ExtremeSecurity Installation Guide*
- *Extreme Networks Security Juniper NSM Plug-in User Guide*
- *ExtremeSecurity Log Manager Administration Guide*
- *ExtremeSecurity Log Manager Users Guide*
- *Migrating ExtremeSecurity Log Manager to Extreme SIEM*
- *ExtremeSecurity Managing Log Sources Guide*
- *ExtremeSecurity Offboard Storage Guide*
- *ExtremeSecurity Release Notse*
- *ExtremeSecurity Risk Manager Adapter Configuration Guide*
- *ExtremeSecurity Risk Manager Getting Started Guide*
- *ExtremeSecurity Risk Manager Installation Guide*
- *ExtremeSecurity Troubleshooting System Notifications Guide*
- *ExtremeSecurity Upgrade Guide*
- *ExtremeSecurity Vulnerability Manager User Guide*
- *ExtremeSecurity Vulnerability Assessment Configuration Guide*
- *ExtremeSecurity WinCollect User Guide*

# 1 Extreme SIEM overview

---

Log activity  
Network activity  
Assets  
Offenses  
Reports  
Data collection  
Extreme SIEM rules  
Supported web browsers

Extreme SIEM is a network security management platform that provides situational awareness and compliance support. Extreme SIEM uses a combination of flow-based network knowledge, security event correlation, and asset-based vulnerability assessment.

To get started, configure a basic Extreme SIEM installation, collect event and flow data, and generate reports.

## Log activity

---

The **Log Activity** tab displays event information as records from a log source, such as a firewall or router device. Use the **Log Activity** tab to do the following tasks:

- Investigate event data.
- Investigate event logs that are sent to Extreme SIEM in real time.
- Search event.
- Monitor log activity by using configurable time-series charts.
- Identify false positives to tune Extreme SIEM.

## Network activity

---

If the content capture option is enabled, the **Network Activity** tab displays information about how network traffic is communicated and what was communicated. Using the **Network Activity** tab, you can do the following tasks:

- Investigate the flows that are sent to Extreme SIEM in real time.
- Search network flows.
- Monitor network activity by using configurable time-series charts.

## Assets

---

Asset profiles provide information about each known asset in your network, including the services that are running. Asset profile information is used for correlation purposes, which helps to reduce false positives.

Use the **Assets** tab to do the following tasks:

- Search for assets.
- View all the learned assets.
- View identity information for learned assets.
- Tune false positive vulnerabilities.

## Offenses

---

Use the **Offenses** tab to view all the offenses that occur on your network and complete the following tasks:

- Investigate offenses, source and destination IP addresses, network behaviors, and anomalies on your network.
- Correlate events and flows that are sourced from multiple networks to the same destination IP address.
- Go to the various pages of the **Offenses** tab to investigate event and flow details.
- Determine the unique events that caused an offense.

## Reports

---

Extreme SIEM provides default report templates that you can customize, rebrand, and distribute to Extreme SIEM users.

Report templates are grouped into report types, such as compliance, device, executive, and network reports. Use the **Reports** tab to complete the following tasks:

- Create, distribute, and manage reports for Extreme SIEM data.
- Create customized reports for operational and executive use.
- Combine security and network information into a single report.
- Use or edit preinstalled report templates.
- Brand your reports with customized logos. Branding is beneficial for distributing reports to different audiences.
- Set a schedule for generating both custom and default reports.
- Publish reports in various formats.

## Data collection

---

Collected data is categorized into three major sections: events, flows, and vulnerability assessment (VA) information.

### Event data collection

Most log sources send information to Extreme SIEM by using the syslog protocol. Extreme SIEM also supports the following protocols:

- Simple Network Management Protocol (SNMP)
- Java™ database Connectivity (JDBC)



- Security Device Event Exchange (SDEE)

By default, Extreme SIEM automatically detects log sources after a specific number of identifiable logs are received within a certain time frame. After the log sources are successfully detected, Extreme SIEM adds the appropriate device support module (DSM) to the **Log Sources** window in the **Admin** tab.

Although most DSMs include native log sending capability, several DSMs require extra configuration, or an agent, or both to send logs. Configuration varies between DSM types. You must ensure the DSMs are configured to send logs in a format that Extreme SIEM supports. For more information about configuring DSMs, see the [ExtremeSecurity DSM Configuration Guide](#).

Certain log source types, such as routers and switches, do not send enough logs for Extreme SIEM to quickly detect and add them to the Log Source list. You can manually add these log sources. For more information about manually adding log sources, see the [ExtremeSecurity Log Sources User Guide](#).

Collected data is categorized into three major sections: events, flows, and vulnerability assessment (VA) information.

## Flow data collection

By accepting multiple flow formats simultaneously, Extreme SIEM can detect threats and activities that would otherwise be missed by relying strictly on events for information.

Extreme Security QFlow Collectors provide full application detection of network traffic regardless of the port on which the application is operating. For example, if the Internet Relay Chat (IRC) protocol is communicating on port 7500/TCP, a QFlow Collector identifies the traffic as IRC and provides a packet capture of the beginning of the conversation. NetFlow and J-Flow notify you only that port 7500/TCP has traffic without providing any context for what protocol is being used.

Common mirror port locations include core, DMZ, server, and application switches, with NetFlow providing supplemental information from border routers and switches.

Extreme Security QFlow Collectors are enabled by default and require a mirror, span, or tap to be connected to an available interface on the Extreme SIEM appliance. Flow analysis automatically begins when the mirror port is connected to one of the network interfaces on the Extreme SIEM appliance. By default, Extreme SIEM monitors on the management interface for NetFlow traffic on port 2055/UDP. You can assign extra NetFlow ports, if required.

## Vulnerability assessment (VA) information

VA information helps Risk Manager identify active hosts, open ports, and potential vulnerabilities.

Risk Manager uses VA information to rank the magnitude of offenses on your network.

Depending on the VA scanner type, Risk Manager can import scan results from the scanner server or can remotely start a scan.

## Extreme SIEM rules

Extreme SIEM includes rules that detect a wide range of activities, including excessive firewall denies, multiple failed login attempts, and potential botnet activity. For more information about rules, see the [Extreme SIEM Administration Guide](#).

The following list describes the two rule categories:

- Custom rules perform tests on events, flows, and offenses to detect unusual activity in your network.
- Anomaly detection rules perform tests on the results of saved flow or event searches to detect when unusual traffic patterns occur in your network.

### Important



A user with non-administrative access can create rules for areas of the network that they can access. You must have the appropriate role permissions to manage rules. For more information about user role permissions, see the [Extreme SIEM Administration Guide](#).

## Supported web browsers

When you access the ExtremeSecurity 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 ExtremeSecurity products**

Web browser	Supported versions
Mozilla Firefox	38.0 Extended Support Release
64-bit Microsoft™ Internet Explorer with Microsoft™ Edge mode enabled.	11.0
Google Chrome	Version 46

# 2 Getting started with Extreme SIEM deployment

---

## Installing the Extreme SIEM appliance

### The Extreme SIEM appliance

### Extreme SIEM configuration

### Extreme SIEM tuning

To deploy Extreme SIEM, administrators must do the following tasks:

- Install the Extreme SIEM appliance.
- Configure your Extreme SIEM installation.
- Collect event, flow, and vulnerability assessment (VA) data.
- Tune your Extreme SIEM installation.

## Installing the Extreme SIEM appliance

---

Before you install the Extreme SIEM evaluation appliance, ensure that you have:

- Space for a two-unit appliance.
  - Rack rails and shelving (mounted).
  - Optional: a USB keyboard and standard VGA monitor for console access.
- 1 Connect the management network interface to the port labeled Ethernet 1.
  - 2 Plug the dedicated power connections into the rear of the appliance.
  - 3 If you need console access, connect the USB keyboard and standard VGA monitor.
  - 4 If the appliance has a front panel, remove the panel by pushing in the tabs on either side and pulling the panel away from the appliance.
  - 5 Power on the appliance.

## The Extreme SIEM appliance

---

The Extreme SIEM appliance includes four network interfaces. For this evaluation, use the interface that is labeled Ethernet 1 as the management interface.

You can use the three remaining monitoring interfaces for flow collection. The QFlow Collector provides full network application analysis and can perform packet captures on the beginning of each conversation. Depending on the Extreme SIEM appliance, flow analysis automatically begins when a span port or tap is connected to any interface other than Ethernet 1. Extra steps might be required to enable the QFlow Collector component within Extreme SIEM.

For more information, see the [Extreme SIEM Administration Guide](#).



#### Restriction

The Extreme SIEM evaluation appliance has a 50 Mbps limit for flow analysis. Ensure that the aggregate traffic on the monitoring interfaces for flow collection does not exceed 50 Mbps.

## Extreme SIEM configuration

- 1 Ensure that Java™ Runtime Environment (JRE) version 1.7 or 64-bit Runtime Environment for Java™ V7.0 is installed on all desktop systems that you use to access the ExtremeSecurity product user interface.
- 2 Ensure that you are using a supported web browser. See [Supported web browsers](#) on page 10.
- 3 If you use Internet Explorer, enable document mode and browser mode.
  - a In your Internet Explorer web browser, press F12 to open the **Developer Tools** window.
  - b Click **Browser Mode** and select the version of your web browser.
  - c Click **Document Mode** and select **Internet Explorer 7.0 Standards**.
- 4 Log in to the Extreme SIEM user interface by typing the following URL with the IP address of the Extreme Security Console:

`https://IP Address`

### Related Links

[Supported web browsers](#) on page 10

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

## Network hierarchy

Extreme SIEM uses the network hierarchy to do the following tasks:

- Understand network traffic and view network activity.
- Monitor specific logical groups or services in your network, such as marketing, DMZ, or VoIP.
- Monitor traffic and profile the behavior of each group and host within the group.
- Determine and identify local and remote hosts.

For evaluation purposes, a default network hierarchy is included that contains predefined logical groups. Review the network hierarchy for accuracy and completeness. If your environment includes network ranges that are not displayed in the preconfigured network hierarchy, you must add them manually.

The objects that are defined in your network hierarchy do not have to be physically in your environment. All logical network ranges belonging to your infrastructure must be defined as a network object.



#### Note

If your system does not include a completed network hierarchy, then use the **Admin** tab to create a hierarchy specific to your environment.

For more information, see the [Extreme SIEM Administration Guide](#).

## Reviewing your network hierarchy

- 1 Click the **Admin** tab.
- 2 In the navigation pane, click **System Configuration**.
- 3 Click the **Network Hierarchy** icon.
- 4 In the **Name** column, expand **Regulatory\_Compliance\_Servers**.  
If your network hierarchy does not include a regulatory compliance server component, you can use your Mail component for the remainder of this procedure.
- 5 Click the nested **Regulatory\_Compliance\_Servers**.
- 6 Click the **Edit** icon.
- 7 To add compliance servers, follow these steps:
  - a In the **IP/CIDR(s)** field, type the IP address or CIDR range of your compliance servers.
  - b Click the **(+)** icon.
  - c Repeat for all compliance servers.
  - d Click **Save**.
  - e Repeat this process for any other networks that you want to edit.
- 8 On the **Admin** tab menu, click **Deploy Changes**.  
You can automatically or manually update your configuration files with the latest network security information. Extreme SIEM uses system configuration files to provide useful characterizations of network data flows.

## Automatic updates

The Extreme SIEM console must be connected to the Internet to receive updates. If your console is not connected to the Internet, you must configure an internal update server. For information about setting up an automatic update server, see the [Extreme SIEM User Guide](#).

Download software updates from the [Extreme Networks Support Portal](#).

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 extra online help content or updated scripts.

## Configuring automatic update settings

- 1 Click the **Admin** tab.
- 2 In the navigation pane, click **System Configuration**.
- 3 Click the **Auto Update** icon.
- 4 In the navigation pane, click **Change Settings**.
- 5 Select the **Basic** tab.
- 6 In the **Auto Update Schedule** pane, accept the default parameters.

- 7 In the **Update Types** pane, configure the following parameters:
  - a In the **Configuration Updates** list box, select **Auto Update**.
  - b Accept the default values for the following parameters:
    - **DSM, Scanner, Protocol Updates**
    - **Major Updates**
    - **Minor Updates**
- 8 Clear the **Auto Deploy** check box.

By default, the check box is selected. If the check box is not selected, a system notification is displayed on the **Dashboard** tab to indicate that you must deploy changes after updates are installed.
- 9 Click the **Advanced** tab.
- 10 In the **Server Configuration** pane, accept the default parameters.
- 11 In the **Other Settings** pane, accept the default parameters.
- 12 Click **Save** and close the **Updates** window.
- 13 On the toolbar, click **Deploy Changes**.

## Collecting events

By collecting events, you can investigate the logs that are sent to Extreme SIEM in real time.

- 1 Click the **Admin** tab.
- 2 In the navigation pane, click **Data Sources > Events**.
- 3 Click the **Log Sources** icon.
- 4 Review the list of log sources and make any necessary changes to the log source.

For information about configuring log sources, see the [ExtremeSecurity Managing Log Sources Guide](#).
- 5 Close the **Log Sources** window.
- 6 On the **Admin** tab menu, click **Deploy Changes**.

## Collecting flows

This procedure is not available for Security Intelligence on Cloud. For more information about how to enable flows on third-party network devices, such as switches and routers, see your vendor documentation.

- 1 Click the **Admin** tab.
- 2 In the navigation menu, click **Data Sources > Flows**.
- 3 Click the **Flow Sources** icon.
- 4 Review the list of flow sources and make any necessary changes to the flow sources.

For more information about configuring flow sources, see the [Extreme SIEM Administration Guide](#).
- 5 Close the **Flow Sources** window.
- 6 On the **Admin** tab menu, click **Deploy Changes**.

## Importing vulnerability assessment (VA) information

By importing VA information, you can identify active hosts, open ports, and potential vulnerabilities.

- 1 Click the **Admin** tab.
- 2 In the navigation menu, click **Data Sources > Vulnerability**.
- 3 Click the **VA Scanners** icon.
- 4 On the toolbar, click **Add**.
- 5 Enter values for the parameters.

The parameters depend on the scanner type that you want to add. For more information, see the [ExtremeSecurity Vulnerability Assessment Configuration Guide](#).



### Important

The CIDR range specifies which networks Extreme SIEM integrates into the scan results. For example, if you want to conduct a scan against the 192.168.0.0/16 network and specify 192.168.1.0/24 as the CIDR range, only results from the 192.168.1.0/24 range are integrated.

- 6 Click **Save**.
- 7 On the **Admin** tab menu, click **Deploy Changes**.
- 8 Click the **Schedule VA Scanners** icon.
- 9 Click **Add**.
- 10 Specify the criteria for how often you want the scan to occur.

Depending on the scan type, the criteria includes how frequently Extreme SIEM imports scan results or starts a new scan. You also must specify the ports to be included in the scan results.

- 11 Click **Save**.

## Extreme SIEM tuning

Before you tune Extreme SIEM, wait one day to enable Extreme SIEM to detect servers on your network, store events and flows, and create offenses that are based on existing rules.

Administrators can perform the following tuning tasks:

- Optimize event and flow payload searches by enabling a payload index on the **Log Activity** and **Network Activity Quick Filter** property.
- Provide a faster initial deployment and easier tuning by automatically or manually adding servers to building blocks.
- Configure responses to event, flow, and offense conditions by creating or modifying custom rules and anomaly detection rules.
- Ensure that each host in your network creates offenses that are based on the most current rules, discovered servers, and network hierarchy.

## Payload indexing

To optimize the **Quick Filter**, you can enable a payload index **Quick Filter** property.

Enabling payload indexing might decrease system performance. Monitor the index statistics after you enable payload indexing on the **Quick Filter** property.

For more information about index management and statistics, see the [Extreme SIEM Administration Guide](#).

## Enabling payload indexing

- 1 Click the **Admin** tab.
- 2 In the navigation pane, click **System Configuration**.
- 3 Click the **Index Management** icon.
- 4 In the **Quick Search** field, type the following:  
`quick filter`
- 5 Right-click the **Quick Filter** property that you want to index.
- 6 Click **Enable Index**.
- 7 Click **Save**.
- 8 Click **OK**.
- 9 To disable a payload index, choose one of the following options:
  - Click **Disable Index**.
  - Right-click a property and select **Disable Index** from the menu.

For detailed information about the parameters that are displayed in the **Index Management** window, see the [Extreme SIEM Administration Guide](#).

## Servers and building blocks

To ensure that the appropriate rules are applied to the server type, you can add individual devices or entire address ranges of devices. You can manually enter server types, that do not conform to unique protocols, into their respective Host Definition Building Block. For example, adding the following server types to building blocks reduces the need for further false positive tuning:

- Add network management servers to the **BB:HostDefinition: Network Management Servers** building block.
- Add proxy servers to the **BB:HostDefinition: Proxy Servers** building block.
- Add virus and Windows™ update servers to the **BB:HostDefinition: Virus Definition and Other Update Servers** building block.
- Add vulnerability assessment (VA) scanners to the **BB-HostDefinition: VA Scanner Source IP** building block.

The Server Discovery function uses the asset profile database to discover several types of servers on your network. The Server Discovery function lists automatically discovered servers and you can select which servers you want to include in building blocks.

For more information about discovering servers, see the [Extreme SIEM Administration Guide](#).

Using Building blocks, you can reuse specific rule tests in other rules. You can reduce the number of false positives by using building blocks to tune Extreme SIEM and enable extra correlation rules.



## Adding servers to building blocks automatically

- 1 Click the **Assets** tab.
- 2 In the navigation pane, click **Server Discovery**.
- 3 In the **Server Type** list, select the server type that you want to discover.  
Keep the remaining parameters as default.
- 4 Click **Discover Servers**.
- 5 In the **Matching Servers** pane, select the check box of all servers you want to assign to the server role.
- 6 Click **Approve Selected Servers**.



### Remember

You can right-click any IP address or host name to display DNS resolution information.

## Adding servers to building blocks manually

- 1 Click the **Offenses** tab.
- 2 In the navigation pane, click **Rules**.
- 3 In the **Display** list, select **Building Blocks**.
- 4 In the **Group** list, select **Host Definitions**.  
The name of the building block corresponds with the server type. For example, **BB:HostDefinition: Proxy Servers** applies to all proxy servers in your environment.
- 5 To manually add a host or network, double-click the corresponding Host Definition Building Block appropriate to your environment.
- 6 In the **Building Block** field, click the underlined value after the phrase **and when either the source or destination IP is one of the following**.
- 7 In the **Enter an IP address or CIDR** field, type the host names or IP address ranges that you want to assign to the building block.
- 8 Click **Add**.
- 9 Click **Submit**.
- 10 Click **Finish**.
- 11 Repeat these steps for each server type that you want to add.

## Configuring rules

- 1 Click the **Offenses** tab.
- 2 Double-click the offense that you want to investigate.
- 3 Click **Display > Rules**.
- 4 Double-click a rule.  
You can further tune the rules. For more information about tuning rules, see the [Extreme SIEM Administration Guide](#)
- 5 Close the Rules wizard.
- 6 In the **Rules** page, click **Actions**.

- 7 If you want to prevent the offense from being removed from the database after the offense retention period is elapsed, select **Protect Offense**.
- 8 If you want to assign the offense to a Extreme SIEM user, select **Assign**.

## Cleaning the SIM data model

Clean the SIM data model to ensure that each host creates offenses that are based on the most current rules, discovered servers, and network hierarchy.

- 1 Click the **Admin** tab.
- 2 On the toolbar, select **Advanced > Clean SIM Model**.
- 3 Select an option:
  - **Soft Clean** to set the offenses to inactive.
  - **Soft Clean** with the optional **Deactivate all offenses** check box to close all offenses.
  - **Hard Clean** to erase all entries.
- 4 Check the **Are you sure you want to reset the data model?** box.
- 5 Click **Proceed**.
- 6 After the SIM reset process is complete, refresh your browser.

When you clean the SIM model, all existing offenses are closed. Cleaning the SIM model does not affect existing events and flows.

# 3 Getting started in Extreme SIEM

Searching events

Saving event search criteria

Configuring a time series chart

Searching flows

Saving flow search criteria

Creating a dashboard item

Searching assets

Offense Investigations

Example: Enabling the PCI report templates

Example: Creating a custom report based on a saved search

For example, you can search information by using default saved searches in the **Log Activity** and **Network Activity** tabs. You can also create and save your own custom searches.

Administrators can perform the following tasks:

- Search event data by using specific criteria and display events that match the search criteria in a results list. Select, organize, and group the columns of event data.
- Visually monitor and investigate flow data in real time, or perform advanced searches to filter the displayed flows. View flow information to determine how and what network traffic is communicated.
- View all the learned assets or search for specific assets in your environment.
- Investigate offenses, source and destination IP addresses, network behaviors, and anomalies on your network.
- Edit, create, schedule, and distribute default or custom reports.

## Searching events

- 1 Click the **Log Activity** tab.
- 2 On the toolbar, select **Search > New Search**.
- 3 In the **Time Range** pane, define the time range for the event search:
  - a Click **Recent**.
  - b In the **Recent** list, select **Last 6 Hours**.
- 4 In the **Search Parameters** pane, define the search parameters:
  - a In the first list, select **Category**.
  - b In the second list, select **Equals**.
  - c In the **High Level Category** list, select **Authentication**.
  - d In the **Low Level Category** list, accept the default value of **Any**.
  - e Click **Add Filter**.
- 5 In the **Column Definition** pane, select **Event Name** in the **Display** list.

- 6 Click **Search**.

#### Related Links

[Example: Creating a custom report based on a saved search](#) on page 23

You can create reports by importing a search or creating custom criteria.

## Saving event search criteria

- 1 Click the **Log Activity** tab.
- 2 On the toolbar, click **Save Criteria**.
- 3 In the **Search Name** field, type **Example Search 1**.
- 4 In the **Timespan** options pane, click **Recent**.
- 5 In the **Recent** list, select **Last 6 Hours**.
- 6 Click **Include in my Quick Searches**.
- 7 Click **Include in my Dashboard**.  
If **Include in my Dashboard** is not displayed, click **Search > Edit Search** to verify that you selected **Event Name** in the **Column Definition** pane.
- 8 Click **OK**.

Configure a time series chart. For more information, see [Configuring a time series chart](#) on page 20.

#### Related Links

[Configuring a time series chart](#) on page 20

You can display interactive time series charts that represent the records that are matched by a specific time interval search.

## Configuring a time series chart

- 1 In the chart title bar, click the **Configure** icon.
- 2 In the **Value to Graph** list, select **Destination IP (Unique Count)**.
- 3 In the **Chart Type** list, select **Time Series**.
- 4 Click **Capture Time Series Data**.
- 5 Click **Save**.
- 6 Click **Update Details**.
- 7 Filter your search results:
  - a Right-click the event that you want to filter.
  - b Click **Filter on Event Name is <Event Name>**.
- 8 To display the event list that is grouped by the user name, select **Username** from the **Display** list.
- 9 Verify that your search is visible on the **Dashboard** tab:
  - a Click the **Dashboard** tab.
  - b Click the **New Dashboard** icon.
  - c In the **Name** field, type **Example Custom Dashboard**.
  - d Click **OK**.
  - e In the **Add Item** list, select **Log Activity > Event Searches > Example Search 1**.

The results from your saved event search display in the Dashboard.

## Related Links

[Saving event search criteria](#) on page 20

You can save specified event search criteria for future use.

## Searching flows

---

- 1 Click the **Network Activity** tab.
- 2 On the toolbar, click **Search > New Search**.
- 3 In the **Time Range** pane, define the flow search time range:
  - a Click **Recent**.
  - b In the **Recent** list, select **Last 30 Minutes**.
- 4 In the **Search Parameters** pane, define your search criteria.
  - a In the first list, select **Flow Direction**.
  - b In the second list, select **Equals**.
  - c In the third list, select **R2L**.
  - d Click **Add Filter**.
- 5 In the **Display** list in the **Column Definition** pane, select **Application**.
- 6 Click **Search**.

All flows with a flow direction of remote to local (R2L) in the last 30 minutes are displayed, grouped, and sorted by the **Application** field.

## Saving flow search criteria

---

- 1 On the **Network Activity** tab toolbar, click **Save Criteria**.
- 2 In the **Search Name** field, type the name **Example Search 2**.
- 3 In the **Recent** list, select **Last 6 Hours**.
- 4 Click **Include in my Dashboard** and **Include in my Quick Searches**.
- 5 Click **OK**.

Create a dashboard item. For more information, see [Creating a dashboard item](#) on page 21.

## Related Links

[Creating a dashboard item](#) on page 21

You can create a dashboard item by using saved flow search criteria.

## Creating a dashboard item

---

- 1 On the **Network Activity** toolbar, select **Quick Searches > Example Search 2**.
- 2 Verify that your search is included in the Dashboard:
  - a Click the **Dashboard** tab.
  - b In the **Show Dashboard** list, select **Example Custom Dashboard**.
  - c In the **Add Item** list, select **Flow Searches > Example Search 2**.

- 3 Configure your dashboard chart:
  - a Click the **Settings** icon.
  - b Using the configuration options, change the value that is graphed, how many objects are displayed, the chart type, or the time range that is displayed in the chart.
- 4 To investigate flows that are currently displayed in the chart, click **View in Network Activity**.

The **Network Activity** page displays results that match the parameters of your time series chart. For more information on time series charts, see [Extreme SIEM User Guide](#).

#### Related Links

[Saving flow search criteria](#) on page 21

You can save specified flow search criteria for future use.

## Searching assets

Use the search feature to search host profiles, assets, and identity information. Identity information provides more details, such as DNS information, user logins, and MAC addresses on your network.

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

You receive a notification that CVE ID: CVE-2010-000 is being actively exploited. To determine whether any hosts in your deployment are vulnerable to this exploit, do the following steps:

- 1 From the list of search parameters, select **Vulnerability External Reference**.
- 2 Select **CVE**.
- 3 To view a list of all hosts that are vulnerable to that specific CVE ID, type the following command:

```
2010-000
```

For more information, see the [Open Source Vulnerability Database](http://osvdb.org/) (http://osvdb.org/) and the [National Vulnerability Database](http://nvd.nist.gov/) (http://nvd.nist.gov/).

## Offense Investigations

---

Extreme SIEM can correlate events and flows with destination IP addresses located across multiple networks in the same offense and the same network incident. You can effectively investigate each offense in your network.

### Viewing offenses

- 1 Click the **Offenses** tab.
- 2 Double-click the offense that you want to investigate.
- 3 On the toolbar, select **Display > Destinations**.

You can investigate each destination to determine whether the destination is compromised or exhibiting suspicious behavior.

- 4 On the toolbar, click **Events**.

The **List of Events** window displays all events that are associated with the offense. You can search, sort, and filter events.

## Example: Enabling the PCI report templates

---

Enable Payment Card Industry (PCI) report templates.

- 1 Click the **Reports** tab.
- 2 Clear the **Hide Inactive Reports** check box.
- 3 In the **Group** list, select **Compliance > PCI**.
- 4 Select all report templates on the list:
  - a Click the first report on the list.
  - b Select all report templates by holding down the Shift key, while you click the last report on the list.
- 5 In the **Actions** list, select **Toggle Scheduling**.
- 6 Access generated reports:
  - a From the list in the **Generated Reports** column, select the time stamp of the report that you want to view.
  - b In the **Format** column, click the icon for report format that you want to view.

## Example: Creating a custom report based on a saved search

---

Create a report that is based on the event and flow searches you created in [Searching events](#) on page 19.

- 1 Click the **Reports** tab.
- 2 In the **Actions** list, select **Create**.
- 3 Click **Next**.

- 4 Configure the report schedule.
  - a Select the **Daily** option.
  - b Select the **Monday, Tuesday, Wednesday, Thursday, and Friday** options.
  - c Using the lists, select **8:00** and **AM**.
  - d Make sure that the **Yes - Manually generate report** option is selected.
  - e Click **Next**.
- 5 Configure the report layout:
  - a In the **Orientation** list, select **Landscape**.
  - b Select the layout with two chart containers.
  - c Click **Next**.
- 6 In the **Report Title** field, type **Sample Report**.
- 7 Configure the top chart container:
  - a In the **Chart Type** list, select **Events/Logs**.
  - b In the **Chart Title** field, type **Sample Event Search**.
  - c In the **Limit Events/Logs To Top** list, select **10**.
  - d In the **Graph Type** list, select **Stacked Bar**.
  - e Click **All data from the previous (24 hours)**.
  - f In the **Base this event report on** list, select **Example Search 1**.

The remaining parameters automatically populate by using the settings from the **Example Search 1** saved search.
  - g Click **Save Container Details**.
- 8 Configure the bottom chart container:
  - a In the **Chart Type** list, select **Flows**.
  - b In the **Chart Title** field, type **Sample Flow Search**.
  - c In the **Limit Flows To Top** list, select **10**.
  - d In the **Graph Type** list, select **Stacked Bar**.
  - e Click **All data from the previous 24 hours**.
  - f In the **Available Saved Searches** list, select **Example Search 2**.

The remaining parameters are automatically populated by using the settings from the **Example Search 2** saved search.
  - g Click **Save Container Details**.
- 9 Click **Next**.
- 10 Click **Next**.
- 11 Choose the report format:
  - a Click the **PDF and HTML** check boxes.
  - b Click **Next**.
- 12 Choose the report distribution channels:
  - a Click **Report Console**.
  - b Click **Email**.
  - c In the **Enter the report destination email address(es)** field, type your email address.
  - d Click **Include Report as attachment**.
  - e Click **Next**.



- 13 Complete the final Report wizard details:
  - a In the **Report Description** field, type a description of the template.
  - b Click **Yes - Run this report when the wizard is complete**.
  - c Click **Finish**.
- 14 Using the list box in the **Generated Reports** column, select the time stamp of your report.

#### Related Links

[Searching events](#) on page 19

You can search for all authentication events that Extreme SIEM received in the last 6 hours.