



Extreme Networks SIEM Getting Started Guide

Copyright © 2015 All rights reserved.

Legal Notice

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

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

Trademarks

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

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

For additional information on Extreme Networks trademarks, please see:

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

Support

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

For information, contact:

Extreme Networks, Inc.
145 Rio Robles
San Jose, California 95134
USA

Table of Contents

- Introduction..... 4**
 - Conventions.....4
 - Providing Feedback to Us..... 5
 - Getting Help.....5
 - Extreme Networks Publications..... 6

- Chapter 1: Extreme SIEM Overview..... 7**
 - Log Activity.....7
 - Network Activity..... 7
 - Assets..... 8
 - Offenses.....8
 - Reports.....8
 - Data Collection.....9
 - Extreme SIEM Rules.....10

- Chapter 2: 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: Using Extreme SIEM.....20**
 - Searching Events.....20
 - Saving Event Search Criteria..... 21
 - Configuring a Time Series Chart.....21
 - Searching Flows.....22
 - Saving Flow Search Criteria.....22
 - Creating a Dashboard Item.....22
 - Searching Assets.....23
 - Offense Investigations.....24
 - Example: Enabling the PCI Report Templates.....24
 - Example: Creating a Custom Report Based on a Saved Search.....24

- Index..... 27**



Introduction

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.

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 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.

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.

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

Extreme Networks Publications

General

Documentation for BlackDiamond Series, E4G, ExtremeXOS, Summit Series, and Ridgeline is available at: www.extremenetworks.com/documentation

Documentation for IdentiFi, NetSight, S/K/7100-Series, SecureStack, Purview, and IPS/SIEM is available at: <https://extranet.extremenetworks.com/downloads/>

Open Source Declaration

Some ExtremeXOS software files have been licensed under certain open source licenses. Information is available at: www.extremenetworks.com/services/osl-exos.aspx

1 Extreme SIEM Overview

Log Activity
Network Activity
Assets
Offenses
Reports
Data Collection
Extreme SIEM Rules

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

In Extreme SIEM, you can monitor and display network events in real time or perform advanced searches.

The **Log Activity** tab displays event information as records from a log source, such as a firewall or router device. Using the **Log Activity** tab, you can 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

In Extreme SIEM, you can investigate the communication sessions between two hosts.

The **Network Activity** tab displays information about how network traffic is communicated, and what was communicated, if the content capture option is enabled. 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

Extreme SIEM automatically creates asset profiles by using passive flow data and vulnerability data to discover your network servers and hosts.

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.

Using the Assets tab, you can do the following tasks:

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

Offenses

In Extreme SIEM, you can investigate offenses to determine the root cause of a network issue.

By using the **Offenses** tab, you can 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.
- Navigate the various pages of the **Offenses** tab to investigate event and flow details.
- Determine the unique events that caused an offense.

Reports

In Extreme SIEM, you can create custom reports or use default 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

Extreme SIEM accepts information in various formats and from a wide range of devices, including security events, network traffic, and scan results.

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

Event Data Collection

Events are generated by log sources such as firewalls, routers, servers, and intrusion detection systems (IDS) or intrusion prevention systems (IPS).

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 *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 *Log Sources User Guide*.

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

Flow Data Collection

Flows provide information about network traffic and can be sent to Extreme SIEM in various formats, including flowlog files, NetFlow, J-Flow, sFlow, and Packeteer.

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.

Behavioral Flow 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 Behavioral Flow 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 there is traffic on port 7500/TCP 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.

Behavioral Flow 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.

Extreme SIEM Rules

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

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 .

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 .

2 Extreme SIEM Deployment

Installing the Extreme SIEM Appliance
The Extreme SIEM Appliance
Extreme SIEM Configuration
Extreme SIEM Tuning

Before you can evaluate Extreme SIEM key capabilities, an administrator must deploy Extreme SIEM.

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

Administrators must install the Extreme SIEM appliance to enable access to the user interface.

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 there is a front panel on the appliance. 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 evaluation appliance is a two-unit rack mount server. Rack rails or shelving are not provided with evaluation equipment.

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 Behavioral Flow 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 Behavioral Flow 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

By configuring Extreme SIEM you can review your network hierarchy and customize automatic updates.

Procedure

- 1 Ensure that following applications are installed on all desktop systems that you use to access the SIEM product user interface:
 - Java™ Runtime Environment (JRE) version 1.7 or IBM® 64-bit Runtime Environment for Java™ V7.0
 - Adobe™ Flash version 10.x
- 2 Ensure that you are using a supported web browser. See [Supported Web Browsers](#).
- 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 SIEM user interface by typing the following URL: `https://<IP Address>`

Where <IP Address> is the IP address of the Extreme SIEM Console.

Network Hierarchy

You can view different areas of your network that is organized by business function and prioritize threat and policy information according to business value risk.

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 pre-configured 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 .

Reviewing Your Network Hierarchy

You can review 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 **Manage Group:Top** list, click **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 **Edit this object** icon.
- 6 To add compliance servers:
 - a In the **IP/CIDR(s)** field, type the IP address or CIDR range of your compliance servers.
 - b Click **Add**.
 - c Repeat for all compliance servers.
 - d Click **Save**.
 - e Repeat this process for any other networks that you want to edit.
- 7 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 Users Guide*.

Using Extreme SIEM, you can either replace your existing configuration files or integrate the updated files with your existing files.

Software updates are available to download from the following website: <http://support.extremenetworks.com/>

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

You can customize the frequency of Extreme SIEM updates, update types, server configuration, and backup 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 In the **Auto Update Schedule** pane, accept the default parameters.
- 6 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.
- 7 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.
- 8 Click the **Advanced** tab.
- 9 In the **Server Configuration** pane, accept the default parameters.
- 10 In the **Other Settings** pane, accept the default parameters.
- 11 Click **Save** and close the **Updates** window.
- 12 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**.
- 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 *Log Sources User Guide*.
- 5 Close the **Log Sources** window.
- 6 On the **Admin** tab menu, click **Deploy Changes**.

Collecting Flows

By collecting flows, you can investigate the network communication sessions between hosts.

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 .
- 5 Close the **Flow Sources** window.
- 6 On the **Admin** tab menu, click **Deploy Changes**.

Importing Vulnerability Assessment Information

By importing vulnerability assessment (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 *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, this 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

You can tune Extreme SIEM to meet the needs of your environment.

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

Use the **Quick Filter** function, which is available on the **Log Activity** and **Network Activity** tabs, to search event and flow payloads.

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 .

Enabling Payload Indexing

You can optimize event and flow payload searches by enabling a payload index on the **Log Activity** and **Network Activity Quick Filter** property.

- 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 **Quick Filter**.
- 5 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 .

Servers and Building Blocks

Extreme SIEM automatically discovers and classifies servers in your network, providing a faster initial deployment and easier tuning when network changes occur.

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 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 .

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

You can automatically add servers to building blocks.

- 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.
Leave 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

If a server is not automatically detected, you can manually add the server to its corresponding Host Definition Building Block.

- 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 **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

From the **Log Activity**, **Network Activity**, and **Offenses tab**, you can configure rules or building blocks.

- 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
- 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**.

Related Links

[Extreme SIEM Rules](#) on page 10

Cleaning the SIM Model

Clean the Extreme SIEM 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 Click the required option:
 - Soft Clean** to set the offenses to inactive.
 - Soft Clean** with the optional **Deactivate all offenses** to close all offenses.
 - Hard Clean** to erase all entries.
- 4 Click **Are you sure you want to reset the data model?**
- 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 Using 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

To get started in Extreme SIEM, learn about searching events, flows, and assets. Also learn how to investigate offenses and create reports.

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

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

- 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**.

Saving Event Search Criteria

You can save specified event search criteria for future use.

- 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 21.

Configuring a Time Series Chart

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

- 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.

Searching Flows

You can search, monitor, and investigate flow data in real time. You can also perform advanced searches to filter the displayed flows. View flow information to determine how and what network traffic is communicated.

- 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 6 Hours**.
- 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 6 hours are displayed and sorted by the **Application Name** field.

Saving Flow Search Criteria

You can save specified flow search criteria for future use.

- 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 22.

Creating a Dashboard Item

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

- 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 the *Extreme SIEM Users Guide*.

Searching Assets

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

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.

For example:

- 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 Type 2010-000 to view a list of all hosts that are vulnerable to that specific CVE ID.

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

Offense Investigations

Using the **Offenses** tab, you can investigate offenses, source and destination IP addresses, network behaviors, and anomalies on your network.

Extreme SIEM can correlate events and flows with destination IP addresses located across multiple networks in the same offense, and ultimately the same network incident. This enables you to effectively investigate each offense in your network.

Viewing Offenses

You can investigate each offense in your network.

For example, you can investigate offenses, source and destination IP addresses, network behaviors, and anomalies on your network.

- 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

Using the **Reports** tab, you can enable, disable, and edit the report templates.

In this getting started task, you enable the 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

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

In this getting started task, you create a report that is based on the event and flow searches you created in [Searching Events](#) on page 20.

- 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.

Index

A

assets
 profiles 8
 searching 23

B

building blocks
 adding servers automatically 17
 adding servers manually 17
 overview 16
 tuning servers 16

C

charts
 configuration
 time series 21
configuration
 automatic update settings 14
 SIEM appliance 12
conventions, guide
 notice icons 4
 text 5

D

dashboards
 items
 creating 22
data collection
 events 9
 flows 9
 overview 9

E

events
 collecting 14
 data collection 9
 searching 20
Extreme SIEM appliance
 overview 11

F

filters
 payload indexing 16
flows
 collecting 15
 data collection 9
 searching 22

I

installations

Extreme SIEM appliance 11

L

log activities
 collecting events 14
 event collection 14
 overview 7
 saving search criteria 21
 searching events 20

N

network activities
 overview 7
 saving search criteria 22
 searching flows 22
network hierarchy
 overview 12
 reviewing 13
networks
 flow collection 15

O

offenses
 investigations 24
 overview 8
 viewing 24

P

patches
 configuring automatic updates 14
payload
 indexing
 configuration 16
payload indexing
 enabling 16
 overview 16
 quick filter property 16
 tuning 16

Q

quick filter
 payload indexing 16

R

reports
 example
 creating based on saved search 24
 enabling PCI report templates 24
 overview 8
rules

configuration 18
overview 10

S

searching
 assets 23
 events 20
 flows 22
 saving event search criteria 21
 saving flow search criteria 22
servers
 adding to building blocks
 manually 17
 building blocks
 overview 16
SIM models
 cleaning 18
 updating 18
software updates
 configuring 14

T

time series charts
 configuring 21
tuning
 building blocks 16
 overview 15
 payload indexing 16
 servers 16

V

vulnerabilities assessments
 importing 15