Setting Up a SIEM Update Server

Technical Note

9034346-04

Published November 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

Preface

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, tricks, 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
`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.

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 theExtreme 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 & Threat Protection product documentation listed below can be downloaded from http://documentation.extremenetworks.com.

Extreme Security Analytics

- *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 Downloads & Release Notes*
- *Extreme Security Threat Protection Installation and Configuration Guide*

1 About the SIEM Update Server

If you want to manually manage updates to your SIEM deployment, or if your console is unable to access the Internet, you can set up a SIEM update server to manage the update process.

SIEM uses system configuration files to provide useful characterizations of network data flows. Updates to the system configuration files, available on the Extranet (http://extranet.extremenetworks.com), include minor updates (such as script updates), major updates (such as JAR file updates), or Device Service Module (DSM) updates. Updates also include threat, vulnerability, and geographic information from various security-related websites.

The SIEM Console must be connected to the Internet to receive automatic updates. The auto-update 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 decompress the most current auto-update package to manually update your configuration.

2 Configuring Apache as Your Update Server

You must have an Apache server installed before beginning this procedure.

You can either configure an Apache server or your SIEM Console as your update server. To use your Apache server, follow the steps below. To use your SIEM Console, go to Configuring the SIEM Console as Your Update Server on page 10.

1 Access your Apache server.

2 Create an update directory named `autoupdates/`.

   By default, the update directory is located in the web root directory of the Apache server. You can place the directory in another location if you configure SIEM accordingly. For more information, see the *Extreme Networks SIEM Administration Guide*.

3 Optional: Create an Apache user account and password to be used by the update process.

4 Download the auto-update package from the Extranet.

   a Navigate to the Extreme SIEM downloads page (https://extranet.extremenetworks.com/downloads/Pages/SIEM.aspx).

   b From the **Software** tab, select the latest auto-update package matching your SIEM version.

   c Save the file on your Apache server in the autoupdates directory created above.

5 On the Apache server, type the following command to decompress the auto-update package.

```
tar -zxf updatepackage-[timestamp].tgz
```

6 Configure SIEM to accept updates:

a Log in to the SIEM user interface.

b Click the **Admin** tab.

c From the navigation menu, click **System Configuration**.

d Click **Auto Update**.

e To direct the update process to the Apache server, configure the following parameters in the **Server Configuration** panel:

Webserver	Type the address or directory path of the Apache server.

Note
If the Apache server runs on non-standard ports, add *:<portnumber>* to the end of the address.

Directory	Type the directory location you created in step 2.
Proxy Information -	If proxy information is required to access the Apache server, configure the following parameters: • **Proxy Server** - Type the URL for the proxy server. • **Proxy Port** - Type the port for the proxy server. • **Proxy Username** - Type the necessary username for the proxy server. A username is only required if you are using an authenticated proxy. • **Proxy Password** - Type the necessary password for the proxy server. A password is only required if you are using an authenticated proxy.

f Select the **Deploy changes** check box.

g Click **Save**.

7 Using SSH, log in to SIEM as the root user.

8 To configure the username and password for the Apache server, enter the following commands:

```
/opt/qradar/bin/UpdateConfs.pl -change_username <username>
/opt/qradar/bin/UpdateConfs.pl -change_password <password>
```

The username and password must match those created in step 3.

9 To test your update server, enter the following command:

```
lynx https://<your update server>/<directory path to updates>/manifest_list
```

10 Enter the username and password created in step 3.

If the list of updates is not displayed, contact Customer Support (see Getting Help on page 5).

3 Configuring the SIEM Console as Your Update Server

You can either configure an Apache server or your SIEM Console as your update server. To use your Apache server, follow the steps below. To use your Apache server, go to Configuring Apache as Your Update Server on page 8.

1 Log in to SIEM as the root user.

2 Enter the following command to create the autoupdate directory:

```
mkdir /opt/qradar/www/autoupdates/
```

3 Download the auto-update package from the Extranet.

   a Navigate to the Extreme SIEM downloads page (https://extranet.extremenetworks.com/downloads/Pages/SIEM.aspx).

   b From the **Software** tab, select the latest auto-update package matching your SIEM version.

   c Save the file on your Apache server in the autoupdates directory created above.

4 On your SIEM Console, enter the following command to decompress the autoupdate package.

```
tar -zxf updatepackage-[timestamp].tgz
```

5 Configure SIEM to accept updates:

   a Log in to the SIEM user interface.

   b Click the **Admin** tab.

   c From the navigation menu, click **System Configuration**.

   d Click **Auto Update**.

   e In the **Server Configuration** panel, type `https://localhost/` in the **Winserver** field.

   f If the Send feedback option in the **Update Settings** panel is enabled, clear the check box to disable it.

   g Click **Save and Update Now**.

4 Adding New Updates

After you have configured your update server and set up SIEM to receive updates from the update server, adding new updates only requires you to download updates from the Extranet to your update server.

1 Download the auto-update package from the Extranet.
   a Navigate to the Extreme SIEM downloads page (https://extranet.extremenetworks.com/downloads/Pages/SIEM.aspx).
   b From the Software tab, select the latest auto-update package matching your SIEM version.
   c Save the file on your Apache server in the autoupdates directory created above.
2 Access your update server.
3 Enter the following command to decompress the autoupdate package.

```
tar -zxf updatepackage-[timestamp].tgz
```

4 Log in to SIEM as the root user.
5 Test your update server by entering the following command:

```
lynx https://<your update server>/<directory path to updates>/manifest_list
```

6 Enter the username and password of your update server.

If the list of updates is not displayed, contact Customer Support (see Getting Help on page 5).