Migrating Extreme Security Log Manager to Extreme SIEM

Tech Note for Release 7.1.0 (MR1)

Published July 2015

9034871

Legal Notices

Extreme Networks, Inc., on behalf of or through its wholly-owned subsidiary, Enterasys 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 about Extreme Networks trademarks, go to: www.extremenetworks.com/company/legal/trademarks/

Support

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

Contact

Extreme Networks, Inc.
145 Rio Robles
San Jose, CA 95134
Tel: +1 408-579-2800
Toll-free: +1 888-257-3000

1 Log Manager to Extreme SIEM Migration Tech Note

This technical note provides information on migrating your Extreme Security Log Manager system to Extreme SIEM.

Backup your data before you begin a software migration. For more information on backup and recovery, see the *Extreme Security Log Manager Administration Guide*.

Applying a Extreme SIEM License Key

To migrate your Extreme Security Log Manager software to Extreme SIEM, you must obtain an Extreme SIEM license key.

Before you begin

Download or save the Extreme SIEM license key to your desktop system.

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

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

Procedure

1. Click the Admin tab.
2. On the navigation menu, click System Configuration.
3. From the System Configuration navigation menu, click the System and License Management icon.
4. From the System and License Management window, select the Console containing the Extreme Security Log Manager license key.
5. From the Actions menu, select Manage License.
6. From the Current License Details window, click Browse beside the New License Key File text box.
7. From the File Upload window, locate and select the Extreme SIEM license key.
8. Click Open.
9. Click Save.
10. On the System and License Management window, click Deploy License Key.

Results

The license key information is updated in your deployment.

Added Features

New features are added when Migrating Extreme Security Log Manager to Extreme SIEM.

New features are described in the table below.

Added feature	Description
New Network Activity Tab	Allows you to view and manage network activity on your network.
New Offenses Tab	Allows you to view and manage offenses, which are alerts that notify you of suspicious network or log activity.
Enhanced Rules Tab	Provides new rule tests and responses for testing both network and log activity.
New Assets Tab	Allows you to view and manage assets and vulnerabilities on your network.
Enhanced Reports Tab	Provides additional report types, including Asset Vulnerabilities, Flows, Top Source IPs, Top Destination IPs, and Top Offenses.
Enhanced Dashboard Tab	Allows you to manage multiple dashboard views and provides new dashboard items related to offenses, sources and destinations.

The Internet Threat Information Center dashboard item is not automatically added to your system when you migrate Extreme Security Log Manager to Extreme SIEM. For more information on how to add the Internet Threat Information Center dashboard item, see Adding the Internet Threat Information Center Dashboard Item on page 4.

For more information on using Extreme SIEM, see the *Extreme SIEM Users Guide* and the *Extreme SIEM Administration Guide*.

Adding the Internet Threat Information Center Dashboard Item

The Internet Threat Information Center dashboard item is an embedded RSS feed that provides you with up-to-date advisories on security issues, daily threat assessments, security news, and threat repositories.

Before you begin

This dashboard item is not automatically added when you migrate Extreme Security Log Manager to Extreme Security. You must manually restart the Tomcat service to add the Internet Threat Information Center dashboard item.

NOTE

This procedure assumes that you have already migrated Extreme Security Log Manager to Extreme SIEM.

Procedure to manually restart the Tomcat service

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

Username: root

Password: <password>

2 To restart the Tomcat service, type the following command:

```
service tomcat restart
```

3 Verify that the Internet Threat Information Center dashboard item is displayed on the Dashboard tab:

a Log in to the Extreme Security user interface.

b Click the Dashboard tab.

c From the Show Dashboard list box, select Threat and Security Monitoring.

Results

The Internet Threat Information Center dashboard item will be displayed on the Threat and Security Monitoring dashboard.

Features Changed or Removed

Migrating Extreme Security Log Manager to Extreme Security results in several changes to the interface and customized preferences.

Saved searches

Using Extreme Security Log Manager and Extreme SIEM you can create custom search criteria. The search feature enables you to create saved search criteria to display only the event data matching your search criteria. When you migrate Extreme Security Log Manager to Extreme Security, your saved search criteria is removed.

For more information on saved searches, see the *Extreme SIEM Users Guide*.

Reports Tab

Using Extreme Security Log Manager and Extreme SIEM you can create custom reports. The Report Wizard enables you to generate reports that display data associated with saved search criteria. When you migrate Extreme Security Log Manager to Extreme SIEM, saved custom search criteria is removed, therefore, reports that use the removed custom saved search criteria no longer function.

Previously generated reports are available after migrating Extreme Security Log Manager to Extreme SIEM.

For more information on the Reports tab, see the *Extreme SIEM Users Guide*.

Custom Event Rules

Using Extreme Security Log Manager and Extreme SIEM you can create custom event rules that allow Extreme SIEM to test event logs for suspicious activity. When you migrate Extreme Security Log Manager to Extreme SIEM, your custom event rules are removed.

For more information regarding custom rules, see the Configuring Rules section of the *Extreme SIEM Administration Guide*.